5-2019

Improving Information Sharing: Local Fusion Centers and Their Role in the Intelligence Cycle

Alexis Spall
Pace University, Dyson College of Arts and Sciences

IMPROVING INFORMATION SHARING: LOCAL FUSION CENTERS AND THEIR ROLE IN THE INTELLIGENCE CYCLE

BY: ALEXIS SPALL

SUBMITTED IN PARTIAL FULFILLMENT OF
REQUIREMENTS FOR THE DEGREE OF MASTER OF
ARTS IN MANAGEMENT FOR PUBLIC SAFETY
AND HOMELAND SECURITY
DYSON COLLEGE OF ARTS AND SCIENCES
PACE UNIVERSITY
May 2019

_____
(date)

Abstract

My Master's Project focuses on local fusion centers and the need for improved information sharing practices among law enforcement partners. After the tragic event of September 11th in 2001, the Department of Homeland Security and the Department of Justice recognized a communication gap between law enforcement agencies and a lack of effective information sharing efforts. Fusion centers play a significant role in supporting both criminal and terrorist investigations due to their ability to act as a conduit between various law enforcement partners. Due to their important responsibilities as information sharing hubs that provide valuable analysis and dissemination of information and intelligence, it is essential to enhance information practices among the centers. My Master's Project details a strategy that will assist in advancing information sharing capabilities among local fusion centers to better detect, investigate, mitigate, and avert threats. Specifically, this paper proposes a two-part strategy that entails strengthening current partnerships among fusion centers and law enforcement agencies and developing and implementing a standardized training program for intelligence analysts. Through improved collaborative efforts, fusion centers will be able to better identify, mitigate, and prevent threats to ensure public safety and the security of the country.

Acknowledgments

I would first like to thank my parents, Marcelle and Edward Spall, who have always supported my education and taught me that I can achieve anything with a little hard work. Their interest in my project, endless encouragement, and constant guidance has allowed me to strive to compose this paper. I would also like to thank my brother, Andrew Spall, for his continuous advice and support in all that I endeavor.

I would like to thank my grandparents, Sally and Al Somma, who never forget to tell me how proud they are of me. I can't imagine any better supporters.

I would like to thank my aunt, Doreen Somma-Newsome, who has always offered her help and assistance in my career and education. I thank her for always pushing me to achieve my goals.

I would like to express my very great appreciation and sincere gratitude to my Uncle John, retired NYPD Detective John Petrocelli, who is the reason why I chose this Master's program to begin with. He is also the reason behind my career choice in crime analysis. Because of his advice, I had the opportunity to develop this Master's Project on fusion centers. I thank him for all the times he checked my work and offered valuable insight.

I wish to thank all of my professors at Pace for their helpful guidance, support, and valuable advice for my thesis. Their assistance in developing my project and reviewing my chapters over the course of the program is greatly appreciated.

I would like to express my great appreciation to Professor Cassi Chandler for her assistance and insightful perspectives on intelligence gathering strategies. Her particular knowledge and experience in intelligence has been extremely valuable in composing my project.

Finally, I wish to thank Dr. Ryan and Dr. Long for their valuable advice, constructive suggestions, and constant support in developing my thesis. I thank them for their dedication. I am extremely grateful.

Table of Contents

Chapter 1: Strategy

Introduction

Local intelligence fusion centers provide a unique opportunity for enhancing information sharing among local, state, and federal authorities. By communicating with local, state, and federal authorities, fusion centers are hopefully better able to compile data and identify emerging threats. After identifying threat-related information, fusion centers share the information with local, state and federal governments, and vice versa. Thus, local, state, and federal authorities are better prepared to investigate, and potentially prevent, emerging threats.

Although a few intelligence fusion centers existed prior to September 11th, the Department of Homeland Security (DHS) and the Department of Justice (DOJ) helped to develop several new fusion centers mainly as a response to the tragic event of September 11th (Federal Bureau of Investigation, 2009). Owned and operated by local and state authorities, with the support of federal law enforcement, fusion centers were created to implement unique facilities to serve the purpose of detecting terrorism-related information and sharing the information among local, state, and federal authorities (FBI, 2009). The 9/11 Commission Report dealing with the September 11th tragedy detailed a lack of effective communication among all agencies, from local law enforcement to federal agencies (National Commission on Terrorist Attacks, 2004). By not communicating developing information with each other, law enforcement and government agencies neglected to identify the emerging threat. Had they communicated clearly with each other and shared developing information, they could have detected, and possibly prevented, the attack. As a result, fusion centers were created to serve a critical role in identifying, investigating, analyzing, and sharing emerging threat-related information in an efficient and effective manner.

According to DHS (2017a), there are currently 80 fusion centers in the United States that are positioned in various local communities and states to support law enforcement agencies and the federal government in identifying threat-related information. Although all local fusion centers serve the same purpose of identifying emerging threats and sharing the information with the federal government, as well as other levels of government, there is no standard system in place for fusion centers to operate. The lack of a standard set of operations regarding information sharing makes it difficult for fusion centers to identify, investigate, analyze, and share information among local, state, and federal authorities. In order to help improve information sharing among fusion centers, there must be effective partnerships among the analysts, local law enforcement agencies, and local Joint Terrorism Task Forces (JTTF) as well as the creation of a standardized training program for intelligence analysts.

Support for Strategy

In 2004, the Information Sharing Environment (ISE) was established by the President and Congress. Its purpose was to create a trusted partnership among all levels of government, as well as the private sector and foreign partners, to detect, prevent, and mitigate the effects of terrorist threats against the United States. The partnership established under the ISE enabled the appropriate exchange of terrorism-related information among five communities. The communities included intelligence, law enforcement, defense, homeland security, and foreign affairs. The exchange entailed securing timely and accurate information among the aforementioned communities combating terrorism (Department of Justice, 2008).

As part of the National Strategy for Information Sharing, the federal government promoted the use of local fusion centers in order to create an integrated network of facilities that fosters information sharing. The federal government helps to sustain the centers through grant

funding, training, and technical assistance. Through the ISE, fusion centers enable effective communication of locally generated terrorism-related information, such as incident reports and suspicious activity, to government agencies, other fusion centers, and local law enforcement. Communicating with other localities enables fusion centers to better prepare information at the local level and distribute the information to the federal and other related government entities (National Security Intelligence, 2007).

Partnerships. Partnerships encourage collaboration and communication. They encourage support between the groups through training, technical assistance, deployment of personnel, access to databases and networks, and sharing of various resources (DOJ, 2008). Integrating resources between fusion centers and law enforcement from the local context creates a national capacity to identify, analyze, and share information in support of efforts to guard the country (Department of Homeland Security, 2017b).

There are several success stories that highlight the importance of partnerships between local fusion centers, local law enforcement agencies, and joint terrorism task forces. In 2009, the Colorado Information Analysis Center aided an investigation of a local missing woman with potential ties to terrorism. After analyzing the investigation report, the analysis center shared the information with the local joint terrorism task force which added to an open federal investigation on the woman. The analysis center continued to cooperate with the joint terrorism task force on the investigation and together they were able to link several other individuals with prior ties to terrorism-related crimes to the missing woman. Based upon the collaborative efforts among the analysis center and joint terrorism task force, the suspect was apprehended and later convicted for providing material support to terrorists (DHS, 2015a).

Another success story took place when a law enforcement officer in San Antonio

reported information of a Minnesota-based hate group to their local fusion center in Southwest Texas subsequent to making contact with an individual who had ties to the group. After reviewing the report and beginning research on the individual and associated hate group, the fusion center informed the joint terrorism task force of San Antonio who then referred the information to both the Minnesota joint terrorism task force and Minnesota Fusion Center. The Minnesota Fusion Center coordinated with local law enforcement in Minnesota to determine if there was a viable domestic threat in their jurisdiction. The following day, with the help of the Minnesota Police Department Bomb Squad, the FBI executed a search warrant of the suspected individual's home, uncovered suspected pipe bombs, Molotov cocktails, and firearms, and eventually arrested the individual (DHS, 2015b).

Training. In addition to partnerships, local fusion centers rely heavily on the capabilities of intelligence analysts. The analysts receive training, coordinated by DOJ and DHS, in order to acquire skills in identifying, collecting, and analyzing information. While analysts have access to training workshops on topics such as risk analysis, privacy rights, and security (DHS, 2017d), it is important that analysts in fusion centers receive standardized training to ensure a common set of capabilities. Developing a common set of proficiencies among all analysts in fusion centers ensures that they receive baseline capabilities for information collection and sharing. It also improves communication among analysts in different fusion centers as they will all have learned about the same intelligence databases and acquired the same knowledge on analysis and dissemination processes.

In 2010 the DOJ documented common analytic competencies that local, state, and tribal intelligence analysts in fusion centers must exhibit. In order to address the necessity of common competencies, the Office of the Director of National Intelligence (ODNI) initiated the State,

Local, and Tribal (SLT) Training Working Group under the support and purview of DHS. Managed by the DHS Office of Intelligence and Analysis (I&A) Mission Support Division (MSD) Intelligence Training Branch, the group researched and consolidated common analytic competencies from previous intelligence analyst and law enforcement training documents that would aid fusion center personnel in developing necessary intelligence proficiencies (DOJ, 2010a).

The efforts accomplished by the SLT Training Working Group, along with members of the Fusion Center Management Group's Technical Assistance and Training Working Group, established a baseline of capabilities for fusion center analysts. The analytical competency areas include thinking critically within the intelligence cycle, sharing information and collaborating, fusing intelligence and law enforcement tradecraft in a homeland security environment, communicating analytic observations and judgements or generating analytic products, and turning concepts and principles into action. Further competencies include accessing sources, anticipating change, establishing trusted networks of key contributors, using software tools to analyze information, producing threat and vulnerability assessments, and evaluating and disseminating suspicious activity reports. Because the analysts may handle both criminal and national intelligence, they have to possess skills, abilities, and knowledge that aids in detecting and investigating various types of intelligence. Their unique environment creates a need for analysts to receive training on specific analytic tradecraft skills that includes the handling, storage, and maintenance of locally generated information, criminal intelligence and a connection to homeland security, and both classified and unclassified intelligence that is generated from the Intelligence Community (DOJ, 2010a).

Furthermore, intelligence analysts in fusion centers are required to gain knowledge on the

intelligence cycle, different types of intelligence, crime-specific training, various tactical, operational, and strategic products, and fusion centers' mission, plans, functions, and procedures. Intelligence analysts must also develop knowledge on different topics related to information regarding both criminal activity and terrorism-related intelligence. Recognizing the links between information related to various criminal activity and terrorism-related intelligence guides analysts in identifying activities that are indicative of precursor behaviors, terrorist activities, and threats (DOJ, 2010a).

Strategy

Strengthening existing partnerships and creating standardized training for intelligence analysts will assist in enhancing information gathering and sharing. While these strategies enable effective information sharing among local fusion centers, several decisions regarding the strategies must still be made.

Partnerships. In order to establish better communication between the different partners, all fusion centers should have a few designated representatives from local law enforcement and local joint terrorism task forces staffed in the centers. While still working in the field for ongoing investigations, the local law enforcement personnel and terrorism task force agents will work out of the fusion centers, side by side the analysts. Having these liaisons work side by side with the analysts allows the representatives to keep the analysts constantly updated on threat-related information that they discover in the field. It also allows the analysts to inform the representatives of developing intelligence so that the representatives can then communicate such developments back to their agencies. Additionally, the representatives assigned to work in the centers should either have a background in analysis or have previously worked closely with intelligence analysts, making it easier to understand technical analysis terms, briefings, and

intelligence reports, thus enabling effective communication between them and the analysts.

Another important aspect in strengthening partnerships includes having monthly, face to face meetings within the local fusion centers. Meetings allow the different partners to speak in person and learn about progress and updates on ongoing cases. Most local law enforcement and local joint terrorism task forces are uniquely situated to remain physically close to local fusion centers (FBI, 2009). These field-based personnel must take advantage of their locations and deploy several officers and agents to meet often in the fusion centers. At the meetings analysts should provide bulletins, briefings, or intelligence products on new cases or information that they discover. Similarly, officers and agents can discuss new leads regarding their cases. The groups should also present new suspicious activity reports (SARs) that are considered a top priority. Overall, the meetings allow analysts and law enforcement personnel to voice communication concerns and remain updated on cases and trends.

Decisions must also be made regarding security clearances of fusion centers and what information, as well as how much, they have access to. Security clearances can include various levels such as Secret-level clearances, Top Secret clearances, and Top Secret-Secure Compartmentalized Information clearances (Masse, O'Neil, & Rollins, 2007). Information classification barriers can often cause delays in processing, investigating, and sharing information. Sponsoring security clearances for non-federal government personnel remains an issue and reciprocity is often a concern among different levels of law enforcement. Failing to recognize another's clearance may at times hinder the other groups from accessing facilities and computer systems (Masse et al., 2007).

Additionally, security is an important element of fusion centers. Security pertains to information, databases, documents, and personnel, and consists of measures such as encryption,

authorization, access control, and confidentiality (DOJ, 2006). Because fusion centers collect and maintain a vast amount of information, it is important to ensure that the information is stored safely and remains safeguarded. When fusion centers partner with local law enforcement and local joint terrorism task forces, several personnel become involved in accessing, utilizing, and sharing secure information. A breach in security may be an unintended consequence, thus potentially compromising several cases. For these reasons, it is vital to ensure that information remains secure. Analysts should remain aware of potential emails that might be embedded with viruses or malware from hackers. In order to determine how best to protect data, data owners must consider both policy and technical concerns (DOJ, 2006).

Training. In addition to strengthening partnerships, decisions must be made regarding the creation and implementation of a standardized training program for intelligence analysts in fusion centers. Standardized training for intelligence analysts in fusion centers should be a three-month program to allot for sufficient time to ensure analysts are proficient in several competencies. First and foremost, analysts must be trained in analysis and dissemination methods. This includes how to develop reports on crime statistics and trends, write bulletins, develop maps for hot spots and patterns, and create intelligence briefings. Next, analysts must learn about several databases and computer systems that they will utilize in their daily routines. Such databases include Excel, Access, mapping programs, systems for law enforcement contacts and incident reports, and more. This also includes procedures regarding the storing and maintenance of information as well as capabilities encompassing social media practices. Lastly, the analysts must be trained on legal regulations regarding collection methods of information. Legal information can include laws and regulations related to the gathering, maintenance, and dissemination of information. Because it is important to identify threats without overstepping

authority and infringing upon privacy rights, training will require analysts to learn what they are legally allowed to collect, as well as the methods required to legally acquire or gain access to certain information (DOJ, 2008).

Discussion

It is envisioned that the proposed two-part strategy will help to improve information sharing among local fusion centers. Part One of the strategy focuses on strengthening and developing partnerships between local fusion centers, local law enforcement agencies, and FBI joint terrorism task forces. Strengthening these partnerships includes improving methods of communication through the staffing of local law enforcement and joint terrorism task force personnel in the centers, implementation of monthly meetings, development of security clearances, and application of precautionary security measures. Part Two of the strategy encompasses creating a standardized training program for intelligence analysts in fusion centers. The training must include skills in analysis and dissemination, knowledge on various databases and computer systems, and the understanding of legal regulations regarding the collection of information.

Conclusion

In order to successfully detect, and possibly prevent threats, it is important to improve information sharing among local fusion centers. Fusion centers must partner with local law enforcement agencies and local FBI joint terrorism task forces to enhance communication and combine analytic and investigative skills. Additionally, creating standardized training for fusion center intelligence analysts serves to create uniformity of proficiencies among all fusion centers as well as enhance the capabilities of the analysts in the centers.

When continuing to develop this two-part strategy to enhance information sharing among

fusion centers, several questions regarding my strategy may be raised. How will fusion centers, local law enforcement, and joint terrorism task forces communicate effectively? How will the training for intelligence analysts be funded? And how will managers help to enable and improve information sharing? These questions, along with several others, will be further addressed in the following chapters.

Chapter 2: Management

Introduction

As demonstrated by the tragedy of September 11th, the lack of efficient, consistent information sharing among law enforcement and intelligence agencies led to an unprecedented event that could have been detected, and possibly prevented, had law enforcement and government agencies worked together effectively to recognize warning signs and suspicious activity (Nenneman, 2008). Due to the lack of information sharing capabilities, the Department of Homeland Security and the Department of Justice focused on enhancing information sharing capabilities among fusion centers (Carter & Carter, 2009).

While information sharing capabilities among fusion centers have advanced, it is important to continue to develop partnerships among the analysts, local law enforcement agencies, and joint terrorism task forces as well as create and implement standardized training for intelligence analysts. In order to accomplish this, it is essential to have leaders who will ensure that these strategies are not only developed and implemented in the centers, but that they remain in the centers long term. Fusion centers require managers who will enable effective communication and information sharing among the centers.

Management Theory

While several management theories exist, the open systems approach to management is best suited in enhancing communication within and among local fusion centers, and thus implementing effective information sharing. Originally rooted in biology and social sciences, the concept of general systems evolved as an organizational theory over time. Recognizing similar qualities as other organizational theories, several philosophers and theorists developed general systems as a management practice for organizations (Kast & Rosenzweig, 1972). While often

studied as a closed system that did not interact with its environment, general systems theory evolved to include an open systems perspective in organizations. Open systems theory values communication with the organization's environment as an effective strategy in enhancing work productivity (Kast & Rosenzweig, 1972).

A system is composed of interrelated parts that are interconnected. Systems can either be considered closed or open. While closed systems tend to limit the capabilities of organizations, an open system promotes working with its environment and outside factors in order to be successful. An open system exchanges information, material, or energy with its environment. The system remains in a dynamic relationship with its environment by receiving various inputs, transforming those inputs in some way, and exporting the outputs thereafter. Such a relationship allows the open system to establish a constant flow of information both within the organization and outside the organization. The relationship also allows for feedback between the organization and its environment to fix any issues that may exist (Kast & Rosenzweig, 1972). Feedback entails providing information that reflects the outcomes of acts completed by an individual, group, or an organization (Chikere & Nwoka, 2015).

Rather than reducing an entity into its parts, open system theory emphasizes the relations between the parts. The organization is a system with integrated parts that must coordinate together for efficiency and effectiveness. Internally, those who work inside the organization perform both their individual and group tasks while externally, several transactions exist between the organization and outside institutions. The different parts both within and outside the organization collaborate and work together to ensure success overall. In addition, it is important for individuals within the organization to be aware of the changes that exist in their environment in order to adjust to the changing demands and easily adapt to them. An organization that is not

sensitive to its environment will hardly survive. Technology, social, and economic phenomena are not static. Rather, they are always changing and organizations must adapt in order to survive (Chikere & Nwoka, 2015).

The open systems approach to management consists of several core components. It focuses on cooperation, synergy, and communication in order to exchange necessary information with other subsystems or groups (Von Bertalanffy, 1972). In order to collaborate and work together with other groups to bring about success, the open systems approach to management uses anticipatory control. Anticipatory control entails anticipating errors before they occur. The system often relies on institutions outside the organization so that if a possible error or incident should occur in one part, the other institutions that the organization converses with can aid in mitigating the repercussions. The management theory also takes corrective measures through the managerial functions of planning the goals of the organization, staffing individuals to work within and outside the organization, leading the process of the transformation of products, organizing the final outputs, and controlling the flow of information. Lastly, the theory seeks to continuously improve an organization. Rather than remaining stable, even if the system is already effective, the open systems approach to management requires constant learning and improving to better the organization. Essentially, open systems theory seeks to achieve a dynamic equilibrium (Chikere & Nwoka, 2015).

In order to determine if the open systems management theory is being practiced in modern day organizations, a study was performed on a successful, indigenous organization based in Port Harcourt, Nigeria. The organization was chosen as the case study because it demonstrated similar core components, such as the structure of subsystems and interrelated parts, of the systems theory. The study began with a preliminary survey on the company. The study

population was drawn from a list of three departments within the organization. The respondents who agreed and consented to applying the systems theory of management were further selected for the main study. Thirty questionnaires were administered to the respondents of the three departments. They demonstrated an observable relationship that existed among the departments, or subsystems, that revealed that the components of the organization were connected together. The respondents noted the common flow of communication between the departments and its importance to the success of the organization. The respondents also showed that the organization functioned by often interacting with similar institutions that complemented its efforts and supported the overall success of the organization. Based on the questionnaires and similar traits of the systems theory, the study concluded that the open systems theory was in effect at the organization based in Port Harcourt. The study also recommended that other modern organizations adopt the open systems approach to management to enhance growth and profitability (Chikere & Nwoka, 2015).

In addition to the open systems approach to management, the team leadership model is another valuable management theory in building successful information sharing capabilities among local fusion centers. While there have been several different developments of the team leadership theory, Susan Kogler Hill proposed a team leaderships model that specifically focuses on the ability of the leader to monitor team work and ensure team effectiveness by promoting strong communication and problem solving skills (Northouse, 2012).

Hill’s team leadership model is used to aid leaders who often manage groups with similar capabilities and tasks. It helps leaders determine team issues and concerns, as well as several alternatives to resolve the issues, while remaining cognizant of the team’s capabilities, resources, and external challenges and opportunities. The model allows leaders to be able to work with their

teams within the organization as well as externally, with other groups, outside the organization. Such leaders are able to encourage networking, support, and information sharing with their external environment. They are also able to balance both the internal and external demands placed on their teams as well as to know when to intervene in one or both (Northouse, 2013).

Teams are often complex, dynamic systems that exist in greater systemic contexts of cultures, people, structures, and technologies. As a result, leaders must create synergy within the team and recognize the value in focusing on tasks and people to develop successful team building skills. Task-focused behaviors include work apportionment, goal setting, process structuring, adapting to changes, information seeking, and feedback. Empirical studies often demonstrate that task-focused behaviors relate directly to team effectiveness. Interpersonal skills also contribute greatly to team effectiveness. People-focused behaviors include facilitating team member participation in the group, developing a positive climate, harmonizing problems, setting standards of behavior, and encouraging friendly and supportive behavior. Team leaders must also develop a strong sense of trust among all members and groups to enable constructive feedback and team resiliency (Gerras & Clark, 2011). Such leaders require an abundance of trust, credibility, and competency in order to support their teams (Nenneman, 2008). These qualities combined enable the team leadership model to successfully acquire team effectiveness as well as overall work productivity and success in the organization.

The team leadership model focuses on three broad responsibilities for the leaders to accomplish. First, leaders must enforce efficient productivity and improve the team's ability in accomplishing tasks. This includes focusing on desired goals and outcomes as well as creating certain standards for individual and team performances to be successful in reaching the goals. Second, they must improve the team members' interpersonal skills and intra-team relationships.

In order to accomplish this, team leaders support collaboration among team members, coach them to help improve social skills, and expand team commitment. Third, team leaders must be aware of developing team building skills within the organization as well as contributing to building similar skills outside the organization. External leadership action requires keeping the team connected to its external environment. Keeping the team connected to its environment involves creating strong alliances with outside sources to gain access to information regularly (Northouse, 2013).

Application of Theory to Strategy

The open systems approach to management and the team leadership model provide valuable practices that assist in strengthening partnerships with outside agencies and enforcing training for analysts to support information sharing among fusion centers. By establishing constant communication, networking, and team work with outside agencies, the aforementioned management theories provide fusion centers with the necessary abilities to regularly exchange information with their partners. Similarly, supporting enhancement of capabilities and team productivity for those who share similar tasks and responsibilities supports the need for training for all fusion center analysts.

Challenges. While implementing these strategies to improve information sharing, managers may experience some challenges. Local fusion centers rely heavily on partnerships as part of their system, yet analysts and law enforcement personnel develop and utilize different reports such as briefings, maps, and strategic and tactical products. Additionally, a lack of trusted partnerships and incompatible computer systems and software are often obstacles that can negatively impact the ability to share intelligence efficiently (DOJ, 2006).

Although managers oversee and work with different groups that often perform different

duties, it is their responsibility to create a level of communication that each can understand. Fusion center managers must collaborate with managers from local law enforcement and joint terrorism task forces to assign a few members of these agencies to be staffed within the fusion centers. Staffing the centers with these law enforcement liaisons supports the centers' productivity in communicating and sharing information to better develop intelligence that aids in ongoing efforts to prevent threats.

Additionally, because analysts and law enforcement personal have different access levels and security clearances, having the representatives in the centers allows these personnel to collaborate with one another in gathering information more efficiently and effectively. If certain data is needed regarding imminent threats that analysts may not have access to, they can collaborate with their law enforcement liaisons to access such information. Similarly, the law enforcement representatives can rely on the analysts for access to various databases.

Finally, face to face meetings allow the groups to discuss new information, leads, or cases in detail. Held at the fusion centers, each meeting must consist of a number of analysts, officers, agents, and managers. At the meetings the analysts must present bulletins or briefings on updated information they acquire on possible threats for the officers and agents to follow up on. Analysts should also present intelligence products they create for ongoing investigations. Officers and agents should present new leads or cases they discover in the field in order for analysts to gather information on possible persons of interest or suspects. Either group may also present new suspicious activity reports that are a priority. Ultimately, meetings give each group the opportunity to discuss any communication concerns, updates on emerging threats, and improved methods and techniques to disrupt them. They also help to encourage trust among the partners.

In addition to partnerships, fusion centers rely heavily on the skills of intelligence analysts and their ability to coordinate with each other. There is no standard training system, however, for all analysts in fusion centers to undergo. A lack of unified standards and policies can negatively impact analysts' ability to effectively share information and intelligence (DOJ, 2006). Similarly, if intelligence analysts are not prepared to collect, analyze, and disseminate information, it could adversely impact the quality of intelligence produced and its timely dissemination, ultimately negatively affecting major criminal or terrorism-related cases. Standardized training prepares analysts in gathering and collecting information to avoid such negative consequences (Nenneman, 2008).

Implementing standardized training for intelligence analysts may be a challenge in that it requires determining what should be included in the training. Local fusion centers are built on the capacity of the analysts being able to effectively work together with each other as well as field-based law enforcement personnel (Northouse, 2013). When individual intelligence analysts fail to perform their tasks, the entire group of analysts can be negatively affected (Chikere & Nwoka, 2015). When the entire group fails to effectively accomplish their tasks, there is not enough production of information to share with the other local groups aiding the investigations. As a result, information is not properly gathered, cases are not built, and sharing with federal agencies becomes impossible when there is nothing substantial to share.

Team work and collaboration is a vital element of fusion centers. By creating standardized training, managers are able to foster similar skills, traits, and characteristics of intelligence analysts. A common set of competencies supports better communication, collaboration, and interoperability among the analysts, thus creating effective team work and productivity (DOJ, 2010a). Analysts must acquire skills in analysis and dissemination. They

must gain technical skills and knowledge regarding computer systems and databases. Additionally, they must learn the legal guidelines regarding collection of information and how to store and maintain intelligence. By acquiring the same skills and gaining access to the same systems, analysts are able to easily work with each other and exchange information.

In order to maintain growth of the analysts during and after the training, feedback should be constantly present in and among fusion centers. Feedback allows analysts within different centers to voice concerns, as well as give positive feedback, for continuous growth and development. Managers ensure that feedback remains an integral component for the centers by helping analysts to assess their performances monthly, adapt to changes as necessary, and continue to develop by discussing new ideas to quickly and efficiently prevent viable threats (Morgeson, DeRue, & Karam, 2010).

Lastly, managers must encourage trust among the analysts in the local fusion centers (Morgeson et al., 2010). Building trust helps managers to allow individual analysts to perform their tasks on their own while also knowing when it is necessary to intervene among them. Trust also provides the analysts the ability to easily go to their managers should there be internal, as well as external, problems that could potentially hinder the overall group of analysts and their production in detecting and analyzing threats (Northouse, 2013).

Conclusion

While some challenges may arise when implementing strategies to enhance partnerships among fusion centers and develop standardized training for analysts, managers can help to implement such plans through effective communication. In order to help improve information sharing among local fusion centers, the open systems approach to management and the team leadership model will guide managers in overcoming challenges. Through such practices,

information sharing among fusion centers will be improved, leading to better detection, as well as prevention, of threats to the country.

In Chapter 3, a strategic plan and budget to implement and execute measures for improving information sharing among fusion centers will be proposed. It will address budget issues that may arise when implementing partnerships and intelligence training to enhance information sharing capabilities among local fusion centers.

Chapter 3: Strategic Planning and Budgeting

Introduction

Improving fusion centers' abilities to share information will allow the centers to continue to grow in their capacities to detect and prevent threats. Updating partnerships with local law enforcement and local FBI joint terrorism task forces and developing a standardized training program for intelligence analysts will help to improve information sharing. In order to successfully place this strategy into practice to enhance information sharing among fusion centers, a strategic plan must be developed.

Strategic Planning

When addressing strategy, several components must be considered. Such components include fusion centers' purpose, mandates, stakeholders, vision statement, mission statement, internal & external factors, strategic issues, performance goals, performance indicators, and their budget and resources. These components make up the detailed strategic plan that will assist in enhancing information sharing among fusion centers.

Mandates. Mandates include a description of what an organization has to accomplish based on the services and programs it offers. Mandates are orders or policies that the organization seeks to strive for and carry out. They can be expressed both informally or formally through various methods such as contracts, group expectations, partnership agreements, or policies (Community Literacy of Ontario, 2013). For example, in 2008 the Baseline Capabilities for State and Major Urban Area Fusion Centers was created to supplement Fusion Center Guidelines in order to: 1) establish baseline operation standards for fusion centers and 2) outline the necessary capabilities for fusion centers (DHS, 2017a). These documents are formal mandates of fusion centers.

The main expectation of fusion centers is to keep Americans safe and the country secure by detecting threats before they can become viable. Fusion centers can deliver this expectation by improving information sharing. Each partner involved in the information sharing process plays a vital role. Local law enforcement, local joint terrorism task forces, and analysts must accomplish their individual tasks and then share information they develop with each other to build cases and discover emerging threats. Similarly, the training program for fusion center intelligence analysts provides analysts with the skills necessary to accomplish their individual tasks as well as collaborate with groups and share information more seamlessly.

Stakeholders. Stakeholders are individuals involved in an organization who have either an interest, stake, or claim in the organization, in the activities it partakes in, or how well it performs. Stakeholders are categorized into two groups: inside stakeholders and outside stakeholders. Inside stakeholders comprise those who are closest to the organization and have the most direct claim on the organization's resources. Outside stakeholders include those who neither own the organization nor are employed by it. Rather, outside stakeholders are customers, suppliers, the government, unions, local communities, and/or the public who may still have a general interest in the organization or its activities (Jones, 1994).

Local fusion centers collaborate with several partners including local, state, tribal, territorial, federal, and private sector partners. It is their connection with each of these partners that makes fusion centers unique in conducting analysis, facilitating information sharing, and assisting law enforcement and homeland security professionals in investigating and responding to threats (DHS, 2017a).

For my particular strategy to improve information sharing methods, intelligence analysts, local law enforcement officers, and FBI joint terrorism task force agents are the inside

stakeholders. The analysts gather, analyze, disseminate, and share threat-related information. They create several intelligence products, including intelligence briefings and threat assessments, and perform other tasks including charting, graphing, and mapping (DOJ, 2006). Local law enforcement conduct investigations, follow up on leads, and provide situational awareness of their localities and communities for both the analysts and homeland security partners (DHS, 2017a). This contributes greatly to both the safety of local communities as well as national security. Lastly, local joint terrorism task forces provide expertise on terrorism-related cases. Although managed by the Federal Bureau of Investigation, the task forces consist of federal, state, local, tribunal, and territorial law enforcement partners. Together they are integrated task forces that combat terrorism on both a national and international scale. As a result of their skills and capabilities, their partnership with fusion centers is vital to the success of the centers. They assist in conducting counter-terrorism investigations while providing information for intelligence products and assessments (DHS, 2016).

In addition to inside stakeholders, the main outside stakeholders involved in fusion centers are local communities and the general public. Citizens of the United States have an interest in the activities of fusion centers as the centers seek to keep the country secure and citizens safe from harm. Collaborating with various local law enforcement officials and homeland security partners provides for the safety of the public from criminal and terrorist activity. The general public expects the centers and their law enforcement partners to identify and investigate threats to keep them, and their country, safe.

Vision statement. Vision statements address where an organization is headed in future years and what it seeks to accomplish over time. They should be inspirational whereby the stakeholders of the organization will want to strive for the vision and accomplish the goals

involved (Olsen, 2008). Through information sharing with various law enforcement partners, fusion centers strive to identify, investigate, and prevent serious threats. While fusion centers continue to develop new and efficient ways to share information, they are built on the foundation of detecting threats early and strive to prevent them and protect citizens. They facilitate unique information sharing capabilities to promptly detect all serious threats, and thus prevent such threats and secure Americans' safety (DHS, 2017a).

Mission statement. Mission statements explain what the organization does, who it may do it for, and the purpose of the organization (Johnson, 2010). Fusion centers perform several tasks. They serve as the primary conduit among several partners to continuously exchange information pertaining to investigations. Fusion centers analyze and disseminate threat-related information. Their localities allow them to provide a unique perspective on threats, thus contributing to the national threat picture. They also work with the Department of Homeland Security's Office of Intelligence and Analysis to facilitate the intelligence cycle at the local level and foster information sharing with stakeholders at the federal level (DHS, 2017d). Based on such activities, local fusion centers exist to utilize their skills, expertise, and resources in analysis to share information with law enforcement and maximize their ability to identify, collect, investigate, and respond to criminal and terrorist activity and ensure public safety (DHS, 2017a).

Internal and external situational analysis. In order to ensure that fusion centers are successful, it is essential to analyze the strengths and weaknesses of the organization. A SWOT analysis, consisting of identifying strengths, weaknesses, opportunities, and threats, must be performed to carefully analyze components of fusion centers. The SWOT analysis creates a view of the current state of the organization to aid in determining how best to build its future. The strengths and weaknesses are considered through the internal factors of fusion centers whereby

they have a direct impact on the organization. The opportunities and threats are addressed through external factors, or the environment, of the centers (Olsen, 2013).

The main strengths of fusion centers include the resources, capabilities, and skills they possess. Federal agencies provide numerous resources, including technical support and access to various databases, to fusion centers to support their efforts in detecting threats. Some of the systems and network resources include the Federal Bureau of Investigation's LEO Program, International Criminal Police Organization (INTERPOL), Financial Crimes Enforcement Network (FinCEN), High Intensity Drug Trafficking Areas (HIDTA), and several others (DOJ, 2006). Furthermore, the Department of Homeland Security, along with several other federal partners, provides additional resources through information systems access, training, and guidance (DHS, 2017d).

In addition to resources, fusion centers possess enhanced capabilities. They are equipped to carefully recognize various indicators and warnings. They process and collate information, as well as analyze and disseminate it, to create intelligence products. They also generate risk assessments to identify and prioritize vulnerabilities, threats, and consequences at regular intervals (DOJ, 2008). Their ability to recognize local threats not only impacts local communities but serves to contribute to a greater national security picture. The centers may potentially discover vulnerabilities at the local level that may be related to a much larger plot and threat at the national level (DHS, 2017d).

While fusion centers possess many strengths, one weakness that exists within local fusion centers is difficulty in constantly ensuring effective teamwork amongst analysts. Fusion centers must exhibit strong information sharing abilities, yet it can be difficult to accomplish such goals when analysts often remain isolated at their desks and on their computers, refraining from

collaborating with one another. Fusion centers must foster continuous collaboration among the analysts as working together helps to make a connection between cases or potential suspects quicker, and thus aid in discovering emerging threats sooner.

In addition to strengths and weaknesses, it is important to evaluate external factors of opportunities and threats that may impact fusion centers. An opportunity that stems from the environment of fusion centers involves the collaborative efforts of local law enforcement and federal agencies who provide information to the analysts while working in the field. The goals of fusion centers could not be accomplished without the input from these partners as they contribute greatly to the centers through their unique local perspective and skills. Local officers are familiar with their communities, including the people within them (DHS, 2017a). This allows them to also build a partnership with the private sector and share their resources in investigations. In addition, local joint terrorism task force agents' extensive training, experience, and expertise in terrorism-related cases aid the centers in better identifying suspicious activity that may lead to serious, viable threats (DHS, 2016).

A threat, or challenge, that often emanates from the environment of a fusion center is the lack of effective communication. Fusion centers rely heavily on outside partners to work closely with the analysts in gathering and sharing information to detect threats. It is difficult, however, to constantly and consistently communicate with each partner when they have their own responsibilities. In order to effectively collaborate with outside personnel, the centers need to be able to continuously communicate with them. If something is not understood, the partners must be able to verbalize their concerns and work to correct the issue.

Strategic issues. Strategic issues often emanate from unresolved questions within the organization that require clarification (Ambler, 2017). Addressing these issues and determining

why they are a challenge allows the organization to then determine how best to fix them. While there are several methods in analyzing an organization and determining how to identify its strategic issues, the oval mapping approach is best in identifying the strategic issues of a fusion center. The oval mapping approach consists of utilizing diagrams to better understand concerns that may arise throughout the work production of an organization. It encourages using word and arrow diagrams that include statements on the actions of the organization, how such actions are performed, and the cause and effect relationship among them (Bryson, 2004).

Based upon the number of partners involved in fusion centers and various duties, tasks, and responsibilities that each has, the oval mapping approach is more than fitting for analyzing strategic issues of fusion centers. The diagram can exhibit how the system of a fusion center functions and how each group collaborates with one another. It can also demonstrate how each partner exchanges information. Connecting such dots visually will help fusion centers determine where on the diagrams there may be a concern, especially regarding information sharing practices.

When visualizing the interaction between local law enforcement personnel, joint terrorism task force agents, and intelligence analysts, the main strategic issues identified are communication concerns. For example, differences in security clearances can make it difficult for the partners to access and share certain information. Strategic issues also emanate from inside the centers as intelligence analysts may find difficulty in consistently interacting with one another and fostering teamwork and collaboration. Overcoming these strategic issues of communication and teamwork is a difficult task but one that is necessary for the centers to successfully detect and prevent threats.

Performance goals. Goals in a local fusion center must be specific, measurable,

attainable, responsible, and time specific (Torres, 2014). First and foremost, in order to strengthen and update partnerships, it is vital to acquire a select group of representatives from local law enforcement and local joint terrorism task forces that will act as liaisons in the centers. As a result, it is necessary to develop a liaison selection process. Such a goal includes acquiring, in approximately one year, roughly 10 representatives from local law enforcement and local joint terrorism task force personnel. Depending on the size of the locality and fusion center, more representatives may be acquired, but there should be no more than 25. The representatives are meant to be a small, select groups of local law enforcement and local joint terrorism task force personnel that can work closely with the analysts to collect and share intelligence.

While all local law enforcement and local joint terrorism task force personnel are welcome to apply, there are several required qualities and skills. The applicant must have either a background in analysis or have previously worked closely with intelligence analysts. They must demonstrate exceptional interpersonal and leadership skills. They must also be able to multitask. These skills and qualities will aid greatly in the goals to ease communication between local law enforcement, homeland security partners, and analysts. These representatives are held to a higher standard because they will have numerous responsibilities that require effective information sharing and the ability to act as intermediaries between their groups and the analysts. Lieutenants and sergeants from law enforcement agencies, supervisors from the terrorism task forces, and directors of fusion centers will collaborate together to determine who will be selected to act as liaisons in the centers.

Similar to partnerships, the goals for the standardized training program for fusion center analysts must also be specific, measurable, attainable, responsible, and time specific. Creating and implementing the standardized training program for intelligence analysts in fusion centers

should be completed in approximately two years as it will take time to develop a detailed program, create a selection process, and apply the program to all fusion centers. Individuals applying to fusion centers must exhibit skills and capabilities in either analysis or information technology or have prior experience in such areas. Once hired as analysts, they will undergo the standardized training.

The training program will be three months and consist of three core components. First, the analysts will acquire analysis and dissemination skills, learn how to write intelligence briefings, create graphs and maps, and develop reports that analysts produce daily. Second, they will develop technological skills that include learning about computer systems and databases. This involves storing and maintenance of data. The trainees will also learn how to navigate social media sites efficiently. Lastly, they will study legal regulations in regards to what information they can and cannot collect in the centers. This will ensure information is gathered lawfully.

Performance indicator. In order to ensure that the strategies of fusion centers are successful in detecting and preventing threats, the outcomes of the plan must be measured. There should be several supervisory analysts within the fusion centers who establish performance metrics to determine if the strategies and actions performed in the centers are effective. They must gather previous cases where threats were detected and prevented as a result of the work produced by the centers. They can then analyze the cases, decipher how long it took to first detect the threat, how long it took to investigate, as well as determine if the threat became viable, and understand the methods that were used to avert the threat. They also have to analyze the efforts of each partner, including analysts, local law enforcement personnel, and local FBI joint terrorism task force agents, to determine what could have been done differently to identify the threat sooner. Studying past cases allows these analysts to decipher what the issues were, if there

were any, so that they can be resolved.

Budget and resources. While strategies are vital in improving information sharing, it would be impossible to implement such plans without the necessary resources and budget. Many resources for the partnerships between local law enforcement, local joint terrorism task forces, and analysts currently exist. They each have resources such as databases, various personnel, and computer systems (DHS, 2018d). The additional resources that are necessary, however, primarily include work stations and computers in the fusion centers for the liaisons.

For the second part of my strategy in developing standardized training for analysts in fusion centers, several resources are necessary. It is essential to allocate for the space to train the individuals for the program as well as obtain resources for core components of the training. This includes equipment such as smart boards to present lessons, manuals on intelligence and analysis, computers for the analysts to develop technical skills and navigate various databases, and legal texts and guidelines regarding the gathering and collection of information.

In order to fund these strategies and resources, fusion centers must gain help from the federal government. Currently, the federal government provides both resources and funding to fusion centers to aid in their activities and goals (DHS, 2018c). Specifically, the Department of Homeland Security's Office of Intelligence and Analysis, the Federal Emergency Management Agency, and the Department of Justice provide significant resources, training, and services to fusion centers. Federal agencies also assist in providing grants for various programs and initiatives for the success of fusion centers and their partners (DHS, 2018d). As a result, local fusion centers should look towards the federal government to provide significant assistance in their resources and funding to strengthen partnerships and implement standardized training. Providing such resources and funding, including grants, allows the strategies to improve

information sharing. In turn, the centers can continue to grow and advance in their efforts to effectively share information and better detect and prevent threats.

Effective Communication

Overall, the key to building a successful strategic plan in enhancing information sharing among local fusion centers is establishing effective communication among analysts, law enforcement personnel, and homeland security partners. While communication is a vital component of law enforcement efforts in general, it is especially important to the centers and their ability to effectively integrate and exchange information. Because the centers act as hubs that provide for the receipt, gathering, and distribution of information and intelligence, effective means of communication is essential (DHS, 2017d).

Conclusion

Creating and implementing a strategic proposal requires efficient planning. Such planning includes being able to effectively analyze fusion centers, determine current issues, and how best to resolve them. Detailing my two-part strategy of updating partnerships between local law enforcement, local FBI joint terrorism task forces, and analysts as well as creating and implementing standardized training for fusion center analysts is necessary in order to develop and execute such plans. Through my proposal, fusion centers will be able to enhance information sharing capabilities and ultimately, better detect and disrupt threats to the country.

Chapter 4 involves the United States Constitution and the protections it guarantees to citizens. It will also address any concerns or issues that may emanate from local fusion centers and their activities in relation to the fundamental rights granted in the United States Constitution.

Chapter 4: U.S. Constitution and Ethical Issues

Introduction

By conducting analysis and facilitating information sharing, fusion centers assist law enforcement partners and homeland security personnel in averting, protecting against, and responding to both crime and terrorism (DHS, 2017c). While fusion centers serve to detect and prevent threats, it is also important to ensure that in the process, they abide by the rights of those they seek to protect. The Constitution of the United States guarantees citizens several rights (U.S. Const.). While identifying and preventing threats through information sharing practices, fusion centers must be guided by the Constitution and abide by the rights of citizens.

U.S. Constitution

The Constitution of the United States is a living document that represents independence and nationhood of the United States of America. Within the Constitution, the Bill of Rights makes up the first ten amendments that overall limit governmental power and ensure protection of Americans' individual liberties (U.S. Const.).

The First Amendment ensures freedom of speech, religion, press, the right to peacefully assemble, and petition the government for a redress of grievances (U.S. Const. amend. I). The Second Amendment ensures the right of a well-regulated militia and the right of the people to keep and bear arms (U.S. Const. amend. II). The Third Amendment explains that no soldier shall, in a time of peace or war, be quartered in any house without the consent of the owner of the home (U.S. Const. amend. III). The Fourth Amendment guarantees against unreasonable searches and seizures. More specifically, it is the right of the people to be secure in their houses, persons, effects, and papers against unreasonable searches and seizures. If warrants are obtained they must be based upon probable cause and must clearly describe the place to be searched as

well as the persons or things to be seized (U.S. Const. amend. IV). The Fifth Amendment addresses self-incrimination where no person can be held to answer for crimes unless on an indictment or presentment of a grand jury. It also ensures that no person can be tried twice for the same crime and that due process protects a person from being deprived of life, liberty, and property (U.S. Const. amend. V). The Sixth Amendment guarantees a speedy, fair, and public trial in criminal cases. Every person is entitled to an impartial jury, counsel for their defense, the right to be informed of the accusations against them, and the right to be confronted with the witness(s) against them (U.S. Const. amend. VI). The Seventh Amendment ensures the right to trial by jury in civil cases whereby the facts presented to them can never be reexamined in any other court in the United States (U.S. Const. amend. VII). The Eighth Amendment protects against cruel and unusual punishment. It also protects against excessive bail and fines (U.S. Const. amend. VIII). The Ninth Amendment addresses the enumerated powers and rights in the Constitution whereby such rights cannot be construed to deny others retained by the people (U.S. Const. amend. IX). Lastly, the Tenth Amendment explains that the powers that are not delegated to the United States by the Constitution and that are not prohibited by it to the states are then given to states, or the people (U.S. Const. amend. X). Additionally, extending liberties to the Bill of Rights, the Fourteenth Amendment includes equal protection of the law and ensures that individuals are not deprived of life, liberty, or property without due process (U.S. Const. amend. XIV).

Excluding permissible infringements that apply to many Constitutional rights, it is important to abide by the rights provided in the United States Constitution as they are there to protect individual liberties. While there should be efficient law enforcement efforts to ensure constant protection of the people, it is also vital that in the process of developing such efforts,

Constitutional rights are not violated. Namely, with information gathering and sharing methods practiced by local fusion centers, it is important to ensure that the rights of the people are not being denied in the process. If they are, the information gathering and sharing methods must be amended to ensure Constitutional rights are protected.

Data collection. Fusion centers gather and share information with law enforcement partners (DHS, 2017d). When law enforcement agencies collect information on people, however, there can be several concerns including Constitutional rights of equal protection, freedom of expression, and privacy. Given the amount of data that local fusion centers gather such concerns are magnified. The amount of information collected by fusion centers raises concerns that information may be accessed or stored improperly in databases and that individuals may potentially be subjected to unwarranted scrutiny based on either innocuous activities or their religious or political beliefs or racial status (The Constitution Project, 2012). Additionally, as the centers continue to expand their information collection abilities, there is the potential for accountability and oversight evasion, data breaches regarding the involvement of the private sector, and manipulation of data collection and mining processes that may threaten privacy and negatively impact civil liberties (American Civil Liberties Union, 2019).

Specifically, the Fourth Amendment of the Constitution protects individuals from unreasonable searches and allows individuals to be secure in their persons and houses. Warrants must also be obtained by probable cause (U.S. Const. amend. IV). Suspicious activity reporting is a concept in which law enforcement personnel and homeland security leaders identify and share information that is indicative of preoperational planning regarding criminal activity or terrorism. Fusion centers share these reports with FBI joint terrorism task forces (Nationwide SAR Initiative, n.d.). Such reports, however, may inadvertently infringe upon individual's rights

protected by the Fourth Amendment. Data collection regarding suspicious activity observed by law enforcement officials could potentially result in the creation of vast databases of information compiled on individuals without reasonable suspicion that such individuals are actually linked to criminal activity or terrorism (The Constitution Project, 2012).

In addition to the Fourth Amendment, the First Amendment regarding freedom of speech, religion, and press may be impacted by fusion centers. The amendment guarantees that individuals can express themselves freely and as they choose, such as through their religious and political beliefs. A main concern with fusion centers in relation to the rights provided in the First, as well as the Fourteenth, Amendment of the Constitution is the potential of profiling. Efforts taken by fusion centers to monitor, surveil, and share information about individuals may implicate fundamental Constitutional rights of freedom of speech and religion, as well as freedom of association and equal protection. Targeting individuals for suspicion based on characteristics such as political beliefs, religion, or race violates the freedoms granted to individuals in the U.S. Constitution (The Constitution Project, 2012).

While not explicitly stated, another right that has been inferred and recognized from the Constitution is the right to privacy. The right to privacy is interpreted in several of the first ten amendments of the United States Constitution (Right to Privacy, 2017). While fusion centers serve the purpose of analyzing, disseminating, and sharing threat-related information, some individuals are concerned that fusion centers can infringe upon privacy rights (DHS, 2017d). As technology continues to advance, terrorists become smarter and threats become more likely. As a response, it becomes important for the United States to develop new methods to ensure that Americans are safe and that threats do not become viable. With these new approaches and developments, however, privacy concerns can arise as the balance between maintaining security

of the country and ensuring the right to privacy can be difficult to accomplish.

Particularly, individuals question if fusion centers are lawfully gathering and collecting information when seeking to detect threats. These concerns emanate due to questions concerning exactly what information fusion centers are privy to. In order to detect threats, analysts perform several activities, some of which include researching individuals, as well as their backgrounds, that may be considered a threat or may be involved in criminal or terrorist activities. For example, a main tool utilized by fusion centers to identify and share threats includes the SAR Initiative, or Suspicious Activity Reporting. This suspicious activity reporting initiative is used by the centers to form a national network for gathering and sharing local law enforcement reports that include suspicious and potentially terrorism-related activity. As a result, there is a possibility that the program may infringe upon Constitutional rights of privacy based on the loose definition of suspicious activity, exactly what information is included in the initiative, and how such information is obtained (The Constitution Project, 2012).

Solution. While some citizens remain wary that fusion centers can potentially violate several rights guaranteed by the United States Constitution, measures must be taken to ensure that fusion centers protect individuals while refraining from violating inalienable rights. This includes lawfully gathering information that pertains to serious, potential threats. It is also important to ensure that citizens trust and support fusion centers to keep them safe and keep the country secure. Although currently there is federal guidance to protect against activities such as performing unreasonable searches, profiling, and invading privacy when collecting and sharing data, it is imperative to include more guidance, training, and oversight for fusion center activities (The Constitution Project, 2012).

In order to overcome challenges involving civil liberties, Part-Two of my strategy

involves the creation and implementation of standardized training for analysts. By teaching legal regulations as a core component of the training program, intelligence analysts will know how to lawfully gather and store information from the very beginning of their careers. Teaching legal regulations as a core component of the program also assists in information sharing efforts with local law enforcement and local joint terrorism task forces. Instead of receiving information gathered unlawfully, law enforcement personnel will receive information that can be used to build investigations, prosecute offenders, and prevent threats.

Currently, all fusion centers do not operate in the same manner. Since no two fusion centers are alike regarding information collection regulations and procedures, it is difficult to make sure that all are following the law and not abusing their powers (American Civil Liberties Union, 2019). Standardized training, however, ensures uniformity among all fusion centers in regard to guidelines and practices, helping to ensure that all centers are collecting and gathering data lawfully, and thus protecting individuals' Constitutional rights.

Legislation

Enacted by Congress as a response to September 11th, the Patriot Act was created to enforce new tools and methods to detect and prevent terrorism. In order to improve counter-terrorism efforts, the legislation permits law enforcement personnel to utilize surveillance against more crimes of terror, federal agents to follow sophisticated and advanced terrorists trained to evade detection, law enforcement to conduct investigations without tipping off terrorists, and federal agents to ask a court for an order to obtain business records in cases of national security involving terrorism (DOJ, n.d.c).

In addition, the Patriot Act facilitates information sharing, cooperation, and collaboration among various government agencies in order to better “connect the dots” (DOJ, n.d.c, p. 2). The

act removed major legal barriers that restrict law enforcement officials, intelligence analysts, and national defense communities from coordinating their efforts in protecting the American people and ensuring national security (DOJ, n.d.c).

The Patriot Act also updated the law to reflect new threats and technologies. Under this component of the act, law enforcement officials are granted the ability to obtain a search warrant anywhere a terrorist-related activity takes place and victims of computer hacking are allowed to request assistance from law enforcement in monitoring the "trespassers" (DOJ, n.d.c, p. 2) on their computers. Lastly, the act increased the penalties for those who commit acts of terror. This includes prohibiting the harboring of terrorists, enhancing the maximum penalties for different crimes that are likely to be committed by terrorists, enhancing several conspiracy penalties, punishing terrorist attacks on mass transit systems, punishing bioterrorists, and eliminating the statutes of limitations for certain terrorist crimes as well as lengthening them for others (DOJ, n.d.c).

These tools and activities are beneficial to fusion centers as they provide them with better resources and abilities to identify and investigate terrorism-related threats. Similar to the Information Sharing Environment developed by the Department of Homeland Security to support the sharing of information between law enforcement, intelligence agencies, and the private sector, the Patriot Act enforces information sharing to better identify acts of terrorism before they occur (Hodai, 2013).

Conclusion

While the goal of local fusion centers is to protect citizens and keep the country secure, it is imperative that individuals' Constitutional rights are protected. As technology advances and threats become more serious, the balance between ensuring security and guaranteeing

Constitutional rights becomes difficult to maintain. Nonetheless, America is a country founded on the principals and rights provided in the United States Constitution. When developing strategies to ensure safety for the people and security for the country, measures must be taken to ensure that Constitutional rights are not violated. By keeping Constitutional rights in mind while developing information gathering and sharing practices, fusion centers can accomplish their goals in providing safety for the public while still protecting individuals' fundamental rights.

In Chapter 5, policy analysis of fusion centers will be discussed. It will identify the problems of the centers so that they can be addressed and resolved through policy formulation, policy adoption, policy implementation, and policy evaluation.

Chapter 5: Policy Analysis and Evaluation

Introduction

In order to ensure that the proposed strategy for improving information sharing among fusion centers is effective, an evaluation must be completed on the program. Specifically, an outcome evaluation will assess the program's performance and effectiveness in reaching its goals. The planning and design of the evaluation will be conducted based upon a measurement system of success that will guide the assessment of the program's outcomes.

To analyze the program effectively, several fusion centers that provide information sharing and analysis for major urban areas must be randomly chosen and evaluated as samples. Data on the centers must be collected and an evaluation design must be determined. Additionally, a cost benefit analysis of the program will be conducted. Overall, the planned evaluation will assist in determining the effectiveness of local fusion centers.

Evaluation questions. By understanding the operations of fusion centers, their goals and objectives, and metrics of success, the evaluation will provide insight into the overall effectiveness of my strategy for fusion centers and their information sharing practices. It is also important for the evaluation to address existing issues in fusion centers and determine if the new strategies can fix those concerns. Several questions must be asked when performing the evaluation on local fusion centers. The questions include:

- What are the goals and objectives of local fusion centers?
- What are the metrics of success for a fusion center?
- Are collaborative efforts between the analysts and law enforcement partners establishing seamless information sharing?

- Does the standardized training program enhance intelligence analysts' skills and capabilities in analysis and dissemination? Does it establish uniformity among all fusion centers regarding information sharing policies and procedures?
- Has the center improved in its efforts to consistently share information?
- Has the center improved its ability to detect, investigate, and prevent threats in a timely manner?

Policy Analysis Definition/Literature Review

In order to develop an evaluation system for fusion centers, it is necessary to gain insight from previous research on fusion centers and their performance as information sharing hubs. Reviewing past incidents involving work produced by the centers will aid in gathering information from their efforts, productivity, and overall effectiveness. It also helps to acquire information on past failures or successes of the centers and what factors may have attributed to those results.

Theoretical framework. Fusion centers currently operate with intelligence analysts and several different law enforcement and homeland security partners (Devine, 2014). A standardized training program for fusion center analysts has not yet been created, implemented, or utilized in fusion centers. While a standardized training program has not yet been implemented and does not appear in previous research, fusion centers analysts are required to exhibit certain qualities that ensure they can perform their responsibilities in disseminating intelligence and creating analytic products for investigators.

Previous research on the effectiveness of fusion centers and their information sharing practices yields differing results. Opponents of the centers recognize the massive funds that are allocated to the centers. Additionally, some scholars and government officials remain concerned

that the centers lack productivity and only generate a small number of analytic products related to terrorism. Many scholars have conducted research regarding inefficiencies and failures of local fusion centers. They discovered that the centers have failed to utilize the information available to them to detect terroristic plots in their respective locality. The researchers state that there is a lack of focus on the specific community needs and local crimes in the fusion center's local area. Research also shows that their tactical, rather than strategic, nature inhibits their efforts to gather and analyze intelligence that results in long-term benefits for national security. A few case studies have even shown that the centers hinder federal counterterrorism efforts as opposed to supporting them. A lack of continuity among the centers and their partners also negatively impacts their work productivity. Finally, a lack of metrics for measuring successes, or failures, stems from the absence of federal guidelines and policies for the centers (Devine, 2014).

While the effectiveness of fusion centers has been in question by some scholars and government officials, there are also notable examples in which the facilities have greatly assisted in disrupting criminal activity and preventing terrorists' plots. Some instances whereby the centers have experienced notable successes include assisting in sex trafficking related arrests (DHS, 2015c), disrupting a synthetic drug ring, and combatting transnational drug networks (DHS, 2015d). They have also been involved in providing support to active shooter, money laundering, and homicide investigations (DHS, 2015e).

Additionally, there have been several instances in which state and local fusion centers played crucial roles in the identification, analysis, and dissemination of information in terroristic plots which led to arrests and prevention of large scale attacks on U.S. soil. Law enforcement collaborated with the centers to terminate a plan to detonate explosives on September 11th, 2009 in the New York City subway system. Additionally, intelligence developed by a fusion center in

Massachusetts contributed to the prevention of a terrorist attack in 2011 on the Capitol building and the Pentagon in Washington D.C. that involved airplanes packed with C-4 plastic explosives (Devine, 2014). In 2012, fusion centers were recognized as the "Most Notable Law Enforcement Interdiction, Arrest or Counter-Terrorism Program" (DHS, 2015e, p. 2). In addition to apprehending criminals and preventing criminal and terrorist activity, the centers have aided in saving lives and avoiding noteworthy physical damages and costs (Devine, 2014).

Specific needs to be met by the program. Without an evaluation, it would be impossible to analyze the performance and effectiveness of fusion centers. The evaluation measures the performances of the centers according to their objectives and what they seek to achieve. Thus, in order to be considered successful at the end of the evaluation, the centers must be measured on specific standards that they must meet as information sharing hubs. This includes identifying imminent and emerging threats as they are made, connecting the dots in investigations through constant communication with partners, informing partners of developing information, producing accurate and timely intelligence, and recognizing the national threat picture. It also entails apprehending suspects, coordinating operations to investigate the threat, and collaborating to mitigate and prevent criminal and terrorist activity.

Goals and objectives of the program. Fusion centers have several different goals and objectives. The main objective of fusion centers is to facilitate information sharing among various partners. A recognized need to fill a communication gap after 9/11 led to the importance of the centers and their abilities to practice effective information sharing methods. The goal is to provide a mechanism where all law enforcement, public safety, and even private sector partners at times, can share threat-related information. The objective of fusion centers is to maximize the centers' abilities to detect, disrupt, investigate, and respond to criminal and terrorist activity

(DHS, 2017c). By integrating information sharing in a coherent and efficient manner, fusion centers can better provide for the safety of citizens and security of the nation.

Target population. In an evaluation of a program, the target population is the primary group of people that a product or service is aimed at (Newcomer, Hatry, & Wholey, 2015). With fusion centers, the target population consists of several groups. First and foremost, the centers serve the public. They are facilities that support both the safety of the people and security of the nation. In addition to the public, the target population consists of intelligence analysts, local law enforcement personnel, and local joint terrorism task force agents. These different groups are considered the target population because they are greatly impacted by the new strategies being implemented in the fusion centers. It is not only important to ensure that the public sees the benefits of the new strategies, but it is also essential for the analysts, local law enforcement personnel, and task force agents to want to partake in the new procedures as well.

Policy Evaluation

An evaluation design consists of developing the best possible approaches to take when analyzing the strategies of the program. The evaluation of fusion centers must be developed by analyzing a few, select centers. These centers will be samples to test as they will allow the evaluators to determine whether the implemented strategies have influenced successful performances of the facilities. The evaluation design is comprised of the inputs, processes, and outcomes of fusion centers. It also entails what factors, such as data collection methods and evaluation instruments, will be included in developing the evaluation design and analyzing the program. Lastly, the evaluation must include any potential problems that may result from the program or evaluation itself as it is important to generate accurate findings.

The inter-rater reliability evaluation design measures consistency among raters evaluating

performances of a program. It includes measurements of the extent to which data collectors, or raters, assign the same score to the same variable in a study. Consisting of individuals who are educated on the operations of fusion centers, the inter-rater reliability evaluation design will only be utilized to ensure consistency among the raters measuring the uniformity of fusion centers' processes and performances. The inter-rater reliability method will be used to determine if these educated raters can achieve a high level of agreement on the performances of the fusion centers and if my strategy contributed to successful outcomes (McHugh, 2012).

Evaluation instruments. In order to complete the evaluation process so that the raters can adequately measure the performance of the centers, the variables of the centers must be analyzed. Some variables to consider when evaluating the effect of my strategy on fusion centers should include the specific methods utilized to detect the emerging threat, if detected at all, the applied processes in transferring the information from one partner to the next, and the time frame of investigations. Similarly, certain criteria regarding the performance of the centers must be met. The factors attributing to success will help to evaluate the centers and their efficiency and effectiveness as a program. In order to determine if fusion centers are successful, the following criteria will be used:

- Detection or identification of emerging threat before it becomes viable (i.e. before a terrorist attack is executed)
- Information passed to other partners in a timely fashion (i.e. as soon as a viable lead persists)
- Weekly production and distribution of intelligence or tactical products to other agencies (DHS, 2018e)

- Weekly leads vetted by the centers that result in the enhancement or initiation of an investigation (DHS, 2018e)
- Apprehension of suspects as a result of efforts made by fusion centers and their law enforcement partners
- Prevention of widespread criminal or terrorist acts

Research methods. Gathering useful information for the evaluation of fusion centers can be accomplished through the process of raters by trained observers. Trained observers are individuals who typically have experience in the subject at hand and thus can provide valuable insight on the effectiveness of fusion centers, along with what may or may not be working with them. Such individuals already have several related skills necessary to understand the program and what would make it successful. This data collection method relies on either volunteer efforts or the use of existing personnel. The raters must collect data on the center's primary mission, the quality of analytic products generated, and prior success stories. Raters by trained observers is also a relatively low-cost data collection effort (Newcomer et al., 2015).

Additionally, focus group interviews are another data collection method that can be useful in evaluating fusion centers. Used as a research strategy in gathering information, focus groups are often conducted by a moderator who guides a small group of individuals in answering a set of carefully sequenced questions. The groups allow for more of a conversation where the study participants do not have to reach agreements, but rather provide their insight on the program based on the questions that they are given. The questions continue to hone in on the specific topic more and more, allowing for detailed answers as the interview continues. Such questions help the moderator gain valuable feedback and insight on the program (Newcomer et al., 2015).

The groups participating in the interviews would consist of stakeholders such as intelligence analysts, local law enforcement, and joint terrorism task force personnel as they are all involved in the information sharing processes of the centers and can provide valuable feedback. The benefit of focus groups is that they are not only useful in the evaluation phase of a program but also in the implementation and design phase. These focus groups can help an agency or program identify key factors that need to be addressed or fixed, and how to do so, in order to improve the value and effectiveness of the program (Newcomer et al., 2015).

Cost benefit-analysis. A cost benefit-analysis (CBA) is an effective program evaluation. CBA is most useful when analyzing a program in order to determine whether its total benefits to society exceed its costs. The negative impacts of the program would be considered costs while positive impacts of the program are counted as benefits (Newcomer et al., 2015). Some costs of fusion centers may include concern for privacy rights or authority figures overstepping their boundaries. In addition, there are monetary costs for items such as computers, information technology equipment, and training guides, as well as personnel such as trainers hired for the standardized training program for analysts. On the other hand, there are numerous benefits to fusion enters. Fusion centers serve all of society by protecting them from the threats that they detect and disrupt. Benefits of the centers would include better communication and uniformity regarding regulations and practices among the fusion centers. Additionally, the facilities protect communities, provide situational awareness, inform important decisions, and enhance information sharing among law enforcement and homeland security partners (DHS, 2015b). Their overall benefits involve protecting society and keeping them safe from criminal or terrorist activity.

Limitations. A concern to address regarding the evaluation is how to proceed with the

findings of the study, especially if they render undesirable results. If the study results in problems of efficiency, it will certainly be a concern for the progress of fusion centers. Questions regarding what can be changed or altered to potentially create a beneficial program for fusion centers and how would that plan be implemented will arise. In addition, since many program evaluations are published online for public view, there may be backlash if the results of the evaluation indicate problems of efficiency. In cases like this, the evaluation can still be published, but it is essential to detail why such results may have happened. This is important because it can help to address what factors or details of the program may need to be fixed in order for the program to be effective. There is the potential for the public to gather an understanding of the program, the goals it seeks to acquire, and the hope that new strategies can be formed to achieve those goals.

Conclusion

In order to ensure successful outcomes, the performances of local fusion centers and the impact of my strategy must be evaluated. An efficient evaluation design, along with research and data collection on the centers, will provide insight into the operations of the centers and their abilities as information sharing hubs. Specifically, the inter-rater reliability evaluation design as well as data collection methods including raters by trained observers and focus group interviews will aid in completing a valid and efficient evaluation method to properly assess the effectiveness of the centers.

Chapter 6 will continue to address the development of my strategy regarding information sharing for fusion centers, but it will do so for a different country. Chapter 6 will assess my proposed strategy for one of America’s allies in the Middle East: Saudi Arabia.

Chapter 6: Comparative Governments

Introduction

The fight against terrorism is a constant battle faced by many nations. The threat to the security of various countries, as well as the safety of the people within them, continues to rise as terrorists become more sophisticated in their plans and methods of attack. Due to the rather high concern of terrorism in the 21st century, it is essential for nations to develop tactics and strategies to combat terrorism and ensure national security.

The United States has developed several counterterrorism tactics to build its national security against threats of terrorism. One of the primary methods that the United States has utilized to combat terrorism is the expanded use of intelligence and information sharing through fusion centers. Serving as the primary focal points with local and state environments for the receipt, gathering, analysis, and sharing of threat-related information among local, tribal, territorial, state, and federal partners, fusion centers had previously identified, investigated, and thwarted serious threats, both criminal and terrorist, to the country (DHS, 2017c) (DHS, 2015f).

In addition to implementing counterterrorism measures through the use of fusion centers, the United States collaborates with other nations to combat terrorism. A prominent partner of the U.S. and their efforts to combat terrorism is Saudi Arabia. Saudi Arabia cooperates with the U.S. to strengthen their efforts to avert terrorist attacks and threats that greatly impact their nation. Just as the U.S. has enhanced its national security through the implementation of fusion centers, Saudi Arabia, too, can benefit from creating and implementing fusion centers in their nation. In turn, Saudi Arabia will be better prepared to defend itself against terrorist activity. The global perspective of terrorism in Saudi Arabia, their current counterterrorism efforts, and a proposed counterterrorism strategy will be addressed in order to heighten Saudi Arabia's national security.

Global Perspective on Terrorism

One of the primary terrorist threats that Saudi Arabia faces is from ISIS, also known as Daesh and ISIL. Saudi Arabia is one the main targets of ISIS because it is both the birthplace of Islam as well as home to the Two Holy Mosques. ISIS often targets Saudi Arabia because they perceive the Saudi Arabian government to be un-Islamic and an enemy of theirs that is too closely associated with the West. In the past, ISIS has both inspired and launched lethal attacks in Saudi Arabia that primarily targeted Saudi security forces and Shia residents. Despite several efforts from Saudi Arabia to identify and prevent terrorist attacks, ISIS-affiliated groups were able to plan and execute several attacks to their nation (Department of State, n.d.).

In addition to ISIS, other threats to Saudi Arabia stem from al-Qaeda. Threats from both ISIS and al-Qaeda in the Arabian Peninsula continue as both groups encourage individual acts of terrorism. In total, Saudi Arabia has faced more than 60 terrorist attacks by both ISIS and al-Qaeda, resulting in more than 200 deaths of both citizens and police officers. In addition to their attacks, ISIS continues to recruit and present their missions, ideologies, and activities on social media networks. This use of social media in recruitment has continued to increase significantly over time (Saudi Arabia & Counterterrorism Fact Sheet, 2017).

Impact of terrorism. According to the country reports on terrorism, a total of 34 terrorist attacks occurred in Saudi Arabia in 2016, most of which included suicide bombers. On January 29th 2016, a suicide bomb attack occurred at a mosque in the Eastern Province of Saudi Arabia by a 22-year-old Saudi national. Because of the attack, four worshippers were killed. Additionally, on July 4th 2016, coordinated bombings occurred in three cities across Saudi Arabia. One suicide bomber wounded two security officers after striking near the U.S. Consulate General in Jeddah. Another attack took place on a security post near the Prophet's Mosque in

Medina in which four guards were killed in the process. The third attack occurred near a Shia mosque in the Eastern Province city of Qatif. In this attack, only the bomber was killed. In addition to the attacks themselves, terrorism financing can greatly impact the nation and lead to the execution of the attacks. While Saudi Arabia has sought to maintain supervision of the banking sector and strengthen penalties for financing terrorism, there are still allegations that funds are collected in secret and then illicitly transferred out of the country in cash (Department of State, n.d.).

Organized crime and conflict. Along with terrorism, organized crime plays a significant role in the threats against Saudi Arabia and their stability as a nation. The smuggling of narcotics continues to be a challenge along the border areas. Additionally, the threat of kidnappings by terrorist groups remains as a potential concern as terrorist organizations may begin to resort to targeting individuals rather than carrying out widespread, large-scale attacks. Saudi Arabia has also experienced some cyber threats in recent years. In 2012, Saudi Aramco, Saudi's oil company, fell victim to one of the first, well-documented cyber-attacks that occurred in the Gulf. Other cyber-attacks that happened in 2016 have impacted both the civil aviation and transportation agencies (Saudi Arabia & Counterterrorism April, 2017).

Furthermore, beggars who often work on the streets in Saudi Arabia attempt to raise money and funds for criminal and terrorist activities as they have links to both criminal and terrorist groups that operate both in the Kingdom and abroad. The individuals committing these crimes are largely illegal workers who may have outstayed their Haj and Umrah visas in the country. While the beggars continue to acquire funds in support of their links to the criminal and terrorist groups by begging for donations, studies are showing that many are also seeking to obtain money through social media. Often beggars will provide a bank account on social media

for any individuals who choose to donate. Such practices seem to be appearing more and are potential threats in regard to terrorism financing and funding in Saudi Arabia. While Saudi Arabia has begun to recognize the threats, inform the public of their plans, and work towards preventing the beggars from acquiring funds, it is essential that these acts are prevented altogether. Providing funds for terrorists is one of the main factors that allows them to carry out their acts of terrorism in the first place (Beggars, 2015).

As often seen in various areas in the Middle East, ongoing regional conflict could potentially affect national security for Saudi Arabia. The instability in Iraq and the war in Yemen consistently produce numerous fights and attacks on both the northern and southern borders of Saudi Arabia. Yemen's Houthi militia has launched multiple SCUD missiles into Saudi Arabia. These attacks resulted in severe damage to the land and loss of life of the Saudi people. The combination of the violence that occurs within miles of the border with Yemen as well as an increase in illegal immigration and smuggling from the southern border contributes to a very real threat to Saudi Arabia and its safety and security (Department of State, 2017a).

International Counter-Terrorism Strategies

In 2016, despite the attacks that took place, Saudi Arabia developed initiatives and counterterrorism measures to prevent further incidents. As a result of their efforts, they arrested several terrorist suspects, disrupted active terrorist cells all across the Kingdom, and reinforced their capacity to combat violent extremist ideologies. They also heightened their law enforcement and intelligence efforts in the fight against terrorism (Department of State, n.d.).

Role of law enforcement. Law enforcement officials in Saudi Arabia frequently work directly with the community. They include large numbers of high-profile uniformed and plain-clothed officers who work openly and covertly throughout communities (Department of State,

2017a). Neighborhood police units seek to work with the community in order to encourage citizens to provide information about suspected terrorist activity. Law enforcement authorities also focus highly on preventing terrorism financing. They impose financial sanctions regarding terrorism funding to deter offenders from providing money to terrorists and essentially aiding in their plans of execution. Such sanctions are imposed on any individuals or entities who act on behalf of or provide support for terrorist groups including, but not limited to, Hizballah, al-Qa'ida (AQ), Lashkar e-Tayyiba (LeT), and the Taliban (Department of State, n.d.).

Role of intelligence. When first recognizing the need for intelligence, Saudi Arabia sought to build facilities that could provide information for decision makers and participate with other security services. As a result, Saudi Arabia set up an intelligence service beginning with the opening of an office for intelligence in the year 1376 Hijra, corresponding to 1955, under the name of "Al-Mabahith Al-Aammah," or General Investigations (Saudi Secret Service, 2000-2019). Over time intelligence continued to expand as a valuable source of security and the General Intelligence Presidency became the primary intelligence agency in Saudi Arabia today (Saudi Intelligence Agencies, 2017).

The General Intelligence Presidency (GIP) is tasked with ensuring national security through information analysis. The center reports back to the King of Saudi Arabia providing him with valuable information, assessments, and strategic evaluations. The center is highly important to the country as it is the most accredited advisor to the ruler, giving him insight on potential threats and how best to mitigate them. The GIP consists of several personnel and offices within the center. This includes an Inspector General for protocol, an office for External Relations, and an office for the Presidency. Over time, the Presidency continued to expand and experience numerous developments. They opened offices abroad and set up local branches to cover various

areas of Saudi Arabia. Such branches comprise the Department for Financial and Administrative Affairs, the Department for Communications and Tapping, a Training and Planning Department, a Technical Department, an Operations Department, and an Analysis Department that is sub-divided into different themes such as politics and terrorism. The Director of the GIP is also supported by a deputy. Additionally, the Presidency was reorganized to include qualified personnel with unique expertise in intelligence and national security. The personnel began to undergo training courses in areas such as computer science in order to develop skills for their work and develop their capabilities in technology (Saudi Secret Service, 2000-2019).

The GIP runs both strategic and counter intelligence operations. The center coordinates information collection and intelligence production practices, plans the activities of national intelligence services, and carries out research and studies. They present their findings to decision makers to draw up both internal and external policies built on the intelligence that the Presidency produces. The center also establishes mutual relations with security services of other countries that are considered to be their allies as they preside over the bilateral relationship with outside, foreign intelligence agencies (Saudi Secret Service, 2000-2019) (Saudi Intelligence Agencies, 2017).

While the GIP remains as the most prominent intelligence agency, Saudi Arabia maintains other agencies that make up their intelligence community. They comprise of the National Guard, the Ministry of Defense and Aviation, the Ministry of Interior, and the Ministry of Foreign Affairs. The Ministry of Defense and Aviation retains its own Information and Security department and is tasked with focusing on policing and military intelligence. The Ministry of Interior has its own domestic intelligence agency that remains in charge of the fight against terrorism in Saudi Arabia and lastly, the Ministry of Foreign Affairs acts as the

intermediary between Saudi Arabia and foreign intelligence agencies. It provides both analysis and evaluations on regional affairs. These centers, just as the GIP, report back to the King of Saudi Arabia. The King essentially remains as the Commander in Chief, presiding over these organizations (Saudi Intelligence Agencies, 2017).

Coordination from an international multifaceted approach. In recent years, Saudi Arabia has become one of the leading nations in seeking to combat terrorism and terrorism financing. Saudi Arabia has acknowledged the importance of counterterrorism strategies and in 2014 issued a royal decree on it. The decree on counterterrorism reinforced that acts of terrorism, terrorist organizations, recruitment through social media, and participation in terrorist activity will not be tolerated. Often, the Kingdom presents public education campaigns to discredit the terrorists and condemn their activities. They also monitor their mosques in order to prevent political or religious incitement. In addition to removing any preachers who may advocate for radical ideologies, they send these preachers through programs to re-educate them and rid them of their radical ideologies. Saudi Arabia also works with individuals who are affected by terrorist recruitment and messages by placing them in de-radicalization programs (Saudi Arabia & Counterterrorism Fact Sheet, 2017).

Saudi Arabia retains close ties with international communities. They are members of the Global Coalition to Defeat ISIS, co-leaders of the Counter ISIS Finance Group (CIFG), and a founding member of the Global Counterterrorism Forum. Saudi security professionals continue to participate in various joint programs around the world in order to build counterterrorism tactics. In December of 2015, they established the Saudi-led Islamic Military Alliance to Fight Terrorism where representatives from a total of 39 different countries attended in order to focus

on discussing financial, ideological, military, and media aspects of counterterrorism measures (Department of State, n.d.).

One of the main countries that Saudi Arabia cooperates and collaborates with is the United States. They maintain a strong counterterrorism relationship with the United States and look to them for assistance, if necessary, especially since the Middle East tends to experience a vast amount of terrorist attacks. Overall, however, the relationship is mutual in that both countries view each other as allies and seek to work together to combat terrorism. For example, while the United States has supported Saudi Arabia through restraining Iranian conduct, Saudi Arabia has also aided the States by influencing the modeling of United States' counter-radicalization programs after their own approach (Saudi Arabia & Counterterrorism April, 2017).

In order to ensure the safety of both the Saudi and U.S. citizens within Saudi Arabian territories and abroad, the countries have continued to strengthen their collaborative efforts in the past couple of years. First and foremost, both countries combat terrorism through the joint military and finance task forces that are operated by the two countries. They work closely together to track and close down illicit money-transfer centers that would otherwise allow the terrorists to carry out their plans. Together they strive to defeat Daesh, Al Qaeda, and Iranian-sponsored extremism and expansionism. By sharing information, the United States and Saudi Arabia cooperate with each other in seeking to shut down the funds from western banks to Middle Eastern extremists that finance the terrorists' activities. Saudi Arabia has even developed "fusion cells" where certain partners, namely Saudi Arabian intelligence officials and law enforcement personnel from the U.S., can work together to investigate and interdict both terrorism plots and finances (Saudi Arabia & Counterterrorism April, 2017).

Human Rights Concerns

Similar to human rights guaranteed to individuals in the United States, the Kingdom of Saudi Arabia contains laws that prohibit "unlawful intrusions into the privacy of persons, their homes, places of work, and vehicles" (Department of State, 2017b, p. 20). Law enforcement officials are required to follow certain precautions such as providing search warrants and maintaining records of searches that are conducted on individuals. Based upon such regulations, human rights of privacy apply to Saudi Arabia as they do in America. Intelligence facilities in Saudi Arabia must refrain from overstepping their authority when collecting and sharing data on individuals so that they do not infringe upon privacy rights (Department of State, 2017b).

Proposed Counter-Terrorism Strategy

Although Saudi Arabia has strengthened their counterterrorism efforts through the development of their intelligence facilities, they have yet to advance the General Intelligence Presidency into a fusion center as the United States has. Once the country transforms their main intelligence center, the GIP, into a fusion center, they can then expand their implementation of fusion centers into several intelligence facilities in the nation.

Creation of fusion center. While the GIP in Saudi Arabia exhibits several unique capabilities that allow the center to be a useful tool to national security, Saudi Arabia can certainly benefit from taking the intelligence center and transforming it into a fusion center. In fact, Saudi Arabia seems to be moving in such a direction as they have already established "fusion cells" where intelligence officials and law enforcement personnel, as well as officials from other countries, work together to investigate terrorism plots and financing (Saudi Arabia & Counterterrorism April, 2017). Nonetheless, transforming the General Intelligence Presidency into a fusion center that exhibits unique information sharing capabilities to detect and prevent

threats will enhance Saudi Arabia's ability to protect their people and ensure their national security.

Two-part strategy. First and foremost, in order to transform Saudi Arabia's General Intelligence Presidency into a fusion center, numerous connections with law enforcement partners must be created and maintained. This entails acquiring police officers to work side by side the intelligence analysts in the office of the General Intelligence Presidency. It is essential for law enforcement personnel and intelligence analysts to work together to develop partnerships for the seamless flow of information sharing. When the officers and analysts can share information more seamlessly, they have a higher chance of identifying connections between cases or suspects that may be a high threat to the nation. While there will be a select amount of law enforcement officials in the center to support the analysts and vice versa, they will also provide the analysts with information from officers who remain on the streets and directly converse with the community.

In order to ensure that analysts and law enforcement officers cooperate effectively, there should also be collaborative meetings with partners. National meetings with the intelligence community, government officials, and law enforcement officers must be held monthly. This will help to retain constant communication and cooperation in Saudi Arabia's counterterrorism efforts. These collaborative, intelligence meetings should entail potential threats to be aware of as well as areas of concern where there may need to be an increase in law enforcement presence. The meetings must also encourage feedback from those attending. Participation is essential in gathering information on how best to proceed with keeping the communities safe and establishing security against terrorism in Saudi Arabia.

Once the GIP is developed into a fusion center to enhance information sharing practices,

a standardized training program for the intelligence analysts in the center must be developed. Because intelligence analysts collect information and transform it into valuable intelligence, they also have the responsibility of informing decision makers, such as the King of Saudi Arabia, on potential threats facing the country (DHS, 2017c). As a result of their duties in informing decision makers, they must be able to produce both accurate and timely intelligence. Additionally, because Saudi Arabia and the U.S. often collaborate with one another and share intelligence for counterterrorism purposes, it is valuable for intelligence analysts in Saudi Arabia to undergo similar training requirements as analysts in the U.S. in order to retain similar skills and learn similar procedures for gathering and sharing intelligence (Department of State, n.d.).

To ensure analysts retain the skills necessary from the training program, the program must consist of three months so that they have sufficient time to learn protocols on information gathering, analytic product development, and intelligence sharing. Throughout the program, analysts must focus on three categories of expertise for their role as intelligence analysts defending the national security of Saudi Arabia. First, they must develop expertise in analysis and the development of intelligence briefings, maps, charts, graphs, and threat assessments. Second, analysts must be trained in information technology. Not only does an analyst have to be tech savvy to perform their everyday duties, but as cyber terrorism becomes more prevalent in the 21st century, analysts must also enhance their technological skills. Such sub-categories should include learning about security measures, databases, and how to both store and maintain valuable information. Third, the training program must contain certain protocols and procedures for analysts to follow when serious threats are detected. The system must consist of the steps to take in preventing the threat and how best to inform decision makers. This also includes knowing the laws of Saudi Arabia to avoid infringing upon privacy rights.

Transforming the General Intelligence Presidency of Saudi Arabia into a fusion center will significantly enhance both the safety and security of the nation. The fusion center will not only provide for valuable intelligence but it will encourage and produce effective information sharing. Fostering information sharing is essential in detecting threats, developing leads, apprehending suspects, and preventing threats before they become viable. In this process, the fusion center will become a valuable asset to the government, law enforcement officials, and the general public of Saudi Arabia seeking to remain safe and defend their national security.

Conclusion

While Saudi Arabia has certainly made progress in their counterterrorism efforts in the past several years, the threat of terrorism is always expanding. As terrorists become smarter and more sophisticated in their plans of attack, it is essential that Saudi Arabia develops new procedures to enhance their efforts to combat terrorism. As terrorism has greatly impacted their country, Saudi Arabia has recognized the value in collaborating internationally, namely with the United States as an ally and supporter in preventing terrorism. Just as the development of fusion centers and information sharing capabilities has assisted in detecting and preventing acts of terrorism in the U.S., it can foster similar results for Saudi Arabia. The creation of a fusion center in Saudi Arabia will allow for advanced partnerships and communication efforts between intelligence analysts and law enforcement officials, thus producing seamless information sharing. In addition, it will heighten the abilities of the intelligence analysts to detect threats, analyze information, and produce valuable and efficient intelligence for the Saudi Arabian government. By generating a fusion center based on those already developed in the United States and implementing these strategies, Saudi Arabia will enhance their safety for the public and national security against any and all criminal and terrorist threats.

In the next chapter, Chapter 7, international human rights will be discussed. More specifically, the development of fusion centers in the United States, their information sharing strategies, and their connection to international human rights will be analyzed.

Chapter 7: International Human Rights

Introduction

While developing and improving information sharing capabilities for local fusion centers is beneficial in detecting and preventing threats, it is essential to consider its impact on international human rights. Human rights include rights that are inherent to all human beings. Regardless of any sex, race, ethnicity, religion, or other status, human beings are born free and equal in rights and dignity. The right to life, liberty and security of person are a few rights that are innate to each human being (United Nations, n.d.). Because these rights are innate, it is crucial that the strategies developed to enhance information sharing capabilities among fusion centers do not infringe upon international human rights. By taking precautionary measures to safeguard rights while developing information gathering and sharing methods for fusion centers, the centers can maintain security for the public and protect human rights.

Theoretical Understanding and International Policies

Both the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights are international laws that detail several rights that are universally protected. The Universal Declaration of Human Rights promotes the strengthening of respect for all fundamental freedoms and human rights. Some rights include a fair and public hearing by an impartial tribunal, protection against any arbitrary arrests or cruel punishments, and the right to recognition everywhere as an individual before the law. Additionally, the law explains that no one may be subjected to any arbitrary interference with their privacy, home, or family, nor experience any attacks upon their reputation. It also states that all people are entitled to equal protection against any form of discrimination. The declaration endorses understanding and tolerance among all nations and religious or racial groups for the maintenance of peace (United

Nations, n.d.).

Similarly, in accordance with the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights recognizes the inherent dignity and inalienable rights of all individuals as well as supports and defends human being's political freedoms and economic, social, and cultural rights. Rights incorporated in the covenant include equality before the law, freedom of opinion and expression, and protection of minority rights. It also prohibits arbitrary interference with privacy as well as discrimination and advocacy of both racial or religious hatred (United Nations, 1996-2019).

Human rights and fusion centers. Prominent concepts in human rights include freedom from interference with privacy, equality before the law, and freedom from discrimination (United Nations, n.d.). Not only are these rights fundamental human rights guaranteed to all, but they relate greatly to fusion centers and some concerns for their activities. While local fusion centers intend to protect individuals through information sharing practices to detect and prevent threats, they have to ensure that in the process they do not violate privacy and equality rights.

Freedom from interference with privacy. Privacy is a recognized human right that guarantees freedom from government interference. The Universal Declaration of Human Rights explains that no individual can be subjected to arbitrary interference with their privacy, home, correspondence, or family. Additionally, they cannot be subjected to attacks on their reputation (United Nations, n.d.). While individuals are protected against such interference, many question fusion centers' activities in regard to privacy rights and how much the government may be interfering in their personal lives. As fusion centers integrate and analyze information and intelligence, the apprehension is that the adoption of such proactive approaches in collecting information intrudes upon individuals' privacy (Masse et al., 2007).

Equality before the law. Additionally, the Universal Declaration of Human Rights states that all individuals are equal before the law and receive equal protection under it. Thus, they cannot be discriminated against in any way (United Nations, n.d.). When gathering information and intelligence in fusion centers, it is important that religious, racial, or political profiling does not influence data collection. Due to the amount of data that the centers aggregate, there are concerns that individuals may be subjected to unjustified scrutiny based on innocuous activities, their religious or political beliefs, or racial status (The Constitution Project, 2012).

National Security and Human Rights

When developing strategies for homeland security, there is often a difficult balance between the implementation of public safety strategies and sustaining human rights. The difficulty lies in balancing the protection of innate human rights that are guaranteed to everyone and ensuring safety and security for those same individuals. Not only can my strategy raise some concerns about fusion centers' activities in relation to violating privacy rights or profiling certain individuals, but sharing such information may cause problems for the relationship between fusion centers and the public (DOJ, 2010b). It can lead to distrust and rather than people supporting fusion center efforts to better detect and prevent threats to protect them, they may end up rejecting the centers and their efforts (The Constitution Project, 2012).

In the process of enhancing strategies to protect the public from adverse criminal or terrorist activity, measures must be taken to assure them that their inherent human rights are protected. In order to retain the protection of human rights, fusion centers must enforce data security, accountability and transparency, and effective training. These measures will help to develop procedures to protect rights when collecting and sharing high volumes of sensitive information (The Constitution Project, 2012).

Data security. Data security is essential in fusion centers due to the vast amounts of information that they gather, share, and store. Because in some instances fusion centers access information from databases from other institutions and agencies at the local, state, and federal levels, consistent security of the shared data may be difficult. One way to monitor data security is to enforce audit logs where individuals accessing, storing, and sharing information are checked regularly and are held accountable for their actions. The logs often record network activity including the user making a certain query, the nature of the query itself, and the information accessed in the process. Not only does this process deter users from accessing and using information improperly, but the logs may also protect against intrusion into databases from unauthorized outsiders or hackers (The Constitution Project, 2012).

Accountability and transparency. Often due to the rapid pace of advancements in information technology, as well as the nation's rather limited experience with the centers' concepts, it is difficult for policymakers to truly understand the nature of fusion center activity. The secrecy that exists around the centers also causes concern for public oversight. As a result, fusion centers should first develop clear mission statements that detail the purpose of their activities and the metrics upon which their performances should be evaluated in order for the public to understand the centers' goals. They should also publish the descriptions of their activities, staffing, budgets, and more. The information will have to remain somewhat broad to refrain from posting classified information, but the public will at least be aware of their policies and procedures. Developing such information and making it available to the public creates openness between fusion center personnel and the community. Consequently, the public can gain an understanding of the centers' practices and perhaps gain trust in their activities, thus increasing public cooperation (The Constitution Project, 2012).

Since the databases in fusion centers contain sensitive, personal information, the databases should provide redress for individuals who believe that the systems contain inaccurate information about them. Redress mechanisms are important because individuals subjected to inaccurate information may potentially find themselves subject to repeated, intrusive investigation. An effective redress, however, ensures the accuracy of information stored in fusion center databases and allows for the opportunity for corrective action should errors occur (The Constitution Project, 2012).

Training. Finally, standardized training must include a section on legal regulations in data collection. Training the analysts early on in their careers about the necessary precautions to take when collecting information will help them to develop practices that support human rights. Training analysts on legal regulations regarding data collection and storage will also assist in developing trust among them and the public.

The aforementioned measures to maintain rights while ensuring security strengthen the trust between the public and fusion centers. Rather than the public opposing the operations of the centers due to potential violations of human rights, they can instead support them. They may recognize their efforts to build greater security for the public and defend them against criminal activity and terroristic threats. Additionally, local communities may even aid in fusion centers' efforts and partner with them to assist in reducing crime. By taking measures to protect human rights while enhancing homeland security strategies, fusion centers can start to close the gap between protecting international human rights and ensuring security.

Practical Application of Human Rights Today

Developing information sharing practices among fusion centers by enhancing partnerships and implementing training for intelligence analysts, however, may inadvertently

break international law. Enhancing partnerships leads to an increase in the amount of people that have access to information. It creates a constant, rapid flow of information and intelligence being shared between various partners. In the process of a significant amount of people gathering and sharing personal, sensitive, and classified information, it is easy to inadvertently pass along information not privy to all. Similarly, training analysts in new ways to collect data on individuals can have adverse repercussions as the public can become concerned that certain analysts may utilize those skills to overstep their boundaries, and doing so undetected, when gathering data. The apprehension is that rather than remaining objective, personal biases or opinions may lead to potential profiling, causing discrimination concerns and breaking international laws that ensure equal treatment for all.

International law is not only created to uphold valuable rights for the people, but to ensure security and peace among varying nations (United Nations, n.d.). Breaking international law could greatly comprise innate human rights as well as peace and security between different countries, causing concerns for the safety of the public and security of the United States. For these reasons, fusion centers must operate under Constitutional law while remaining mindful of international law.

Conclusion

While improving strategies for fusion centers, it is imperative that human rights and international laws protecting them are upheld. International laws protect the public and ensure that they retain rights such as protection from unwarranted government interference as well as equality and fair treatment (United Nations, n.d.). Breaking such laws would severely infringe upon the rights of the public, and ultimately cause distrust and conflict between the public and fusion centers.

In order to ensure that human rights are protected when developing strategies for local fusion centers, it is vital to include certain precautionary measures in the strategies. Increased data security, accountability among law enforcement officials and analysts, transparency among the centers' practices, and lessons on legal regulations regarding privacy are a few measures that can be taken to protect human rights (The Constitution Project, 2012). Overall, these precautionary measures develop a sense of trust and dependency among the public and fusion centers. Through such processes, public trust and cooperation can be gained while also strengthening resilience and security.

In Chapter 8, various intelligence gathering strategies and techniques regarding local fusion centers will be addressed. A threat assessment on the nation state of China and its increased intelligence efforts will also be completed.

Chapter 8: Intelligence Gathering Strategies

Introduction

As advancements in technology and the availability and access to information grow, new threats to the United States intelligence community emerge. Such advancements have led to the expansion of cyber threats emanating from hackers, terrorists, and nation states threatening the security of the U.S. and the safety of its people. In particular, China's cyber capabilities continue to excel, expanding their abilities to collect information and intelligence and making them a viable threat to the U.S. and its intelligence community. China's role in developing technological advancements and cyber proficiencies also contribute to their emerging global influence.

As a result of such impending threats from China, United States' local government officials must recognize and anticipate cyber-attacks and enhance U.S. intelligence gathering and sharing strategies to combat them. In order to expand intelligence efforts to combat such threats, local law enforcement must expand coordination with the federal government and the private sector to acquire greater resources and assistance. Such collaborative efforts in intelligence gathering and sharing can be fostered through the use of intelligence fusion centers. Collaborating and coordinating with local fusion centers to gather and share timely and accurate intelligence will assist the U.S. intelligence community in detecting, investigating, and preventing threatening cyberwar activities from China.

Literature Review

The intelligence cycle. The process of gathering valuable intelligence stems from six important steps known as the intelligence cycle. The intelligence cycle is utilized to transform raw information into finished, actionable intelligence used by consumers and decision makers. The six steps of the intelligence cycle include planning and direction, collection, processing and

exploitation, analysis and production, dissemination, and evaluation (Director of National Intelligence, 2011).

Planning and direction includes identifying and understanding the consumer's intelligence requirements in order to plan the following steps accordingly. Collection is the gathering of the raw data, or information, involved in developing the intelligence product. Processing and exploitation consist of transforming the raw information into a comprehensive format for the final product. This stage requires highly skilled and trained individuals, as well as advanced technological systems and equipment, who are capable of converting the raw information into understandable and useable information. The analysis and production phase entails integrating, analyzing, and preparing the information for its final stages to create actionable intelligence. Dissemination is the delivery of the finished product to the consumer who requested the intelligence product. Lastly, the final step of the intelligence cycle is evaluation. As intelligence products are developed, it is essential to acquire feedback and evaluate such feedback to ensure understanding of consumers' evolving information requirements and needs. Following the intelligence cycle and developing actionable intelligence is important as intelligence influences decisions and drives response efforts to various threats (Director of National Intelligence, 2011).

China's historical activities. China has long been involved in cyber espionage within the United States. Hacking from China was first observed in 1999 when Chinese patriotic hackers planted messages on several United States government websites denouncing previous actions made by NATO. After an international dispute in 2001, the patriotic hackers committed similar acts, defacing the White House site as well as numerous other United States websites. The Chinese continued, and advanced their cyber intrusions in 2003 when hackers stole sensitive

data from computers of the United States Department of Defense. The origin of the attack was traced back to southern China and was believed to have stemmed from their army. The hackers also stole data from defense contractors and several other government agencies. The intrusions appeared to start with spear-phishing, a hacking mechanism that includes sending faux emails to acquire confidential information. Throughout this time, China managed to steal government usernames and passwords as well as intellectual property that included Google's source code and proposals for weapons systems. In 2013, the U.S. connected a Chinese espionage group to stealing data, hundreds of terabytes worth, from approximately 141 companies since 2006. The espionage group was ultimately linked to the People's Liberation Army in China, leading to the U.S. indicting the Chinese officers involved in the hacking and economic espionage (Denning, 2017).

Several years ago, Beijing initiated a cyber-enabled industrial attack, stealing intellectual property from the United States to benefit from U.S. companies' innovations in information technology and aerospace. Such cyber intrusions and thefts by China led to significant economic loss in the U.S, leading the U.S. government to threaten sanctions against Chinese officials and companies associated with the cyber thefts. The threat of imposing sanctions ultimately resulted in a negotiated agreement between the U.S. and China in 2015. The agreement established that neither the United States nor China would conduct any cyber theft of intellectual property for commercial advantage. It asserted that hacking private companies for commercial benefits was simply unacceptable. While companies, soon after, recorded steep declines in hacking performances by the Chinese against the United States, Chinese hackings have recently begun to appear again (Laskai & Segal, 2019).

In prior years, the intelligence community in the U.S. had begun to acknowledge China's

potential cyber intrusions made through the company Huawei. Huawei supplies various telecom equipment and is the world's largest producer of such supplies (Muller, 2018). It is a widely known Chinese organization that accumulates a significant amount of revenue per year and maintains several offices worldwide. The company, however, has recently been banned by numerous agencies due to security concerns and espionage threats. Starting in 2010, the U.S. warned both private companies and agencies of the organization advising that they were acting as a proxy for Chinese government espionage (Fazzini, 2018) and there was growing concern that the company's network gear could contain "back doors" allowing Chinese spies to effectively hack into critical network infrastructure. With the threats of the company's equipment being used to spy on the U.S., as well as other countries, the U.S. has recently requested the arrest of a top Huawei executive (Muller, 2018).

Key Threat Assessment

China's intelligence. Historically, China's purpose, definition, and goal of intelligence remained similar to the United States, demonstrating the importance of valuable knowledge in decision making and preventing advances of adversaries that could cause harm. More modern definitions of Chinese intelligence include the importance of gathering information to foster domestic stability, ensure national security, and protect corporate interests in a rather competitive world. Although somewhat similar to the U.S. intelligence uses, intelligence organizations operate in regard to national policy and the country's needs and priorities. Chinese intelligence, as a result, tends to focus more on domestic terrorism, which is typically different from the U.S., as China often has fewer foreign links. Due to the expansion of the Internet and mobile communications in China, Chinese authorities have also increased investment in their internal security (Mattis, 2012).

While previously influenced by intelligence-led policing, in recent years, China began to adopt “public security informatization” (Mattis, 2012, p. 50) indicating the value in integrating public information more closely with police operations. This included developing domestic intelligence gathering and ensuring information management. China formerly directed its officers to focus on information collection regarding social disturbances in order to link and aggregate local and national level databases with personal information from various businesses requiring government name registration. The information provided in such databases would be utilized to automatically generate tasks for the country’s police officers when a person-of-interest would turn up in their jurisdiction. Later, the Chinese integrated such information collection and intelligence practices with public opinion monitoring to influence decision making about actions in the public sphere. In addition to supporting decision making in China, Chinese intelligence is utilized by their military forces to manipulate decision making of adversaries, develop offensive counterintelligence, and improve capabilities to destroy opponents’ technical skills (Mattis, 2012).

Enhancing capabilities. With rapid advancements in technology and the cyber world, China has sought to make improvements regarding the expansion of their cyberwarfare capabilities. More specifically, Chinese leadership has begun to collaborate with the military, corporations, and universities to improve cyber capabilities. In 2017, the Chinese Education Ministry and the Central Cyberspace Affairs Leading Group developed a joint decree formalizing various rules on building first-rate cybersecurity schools. The goal of the plan is to develop approximately four to six world-class cyber security schools in universities in China. Such schools will be utilized solely for training purposes to create cyber experts. After several years of training in school, the students will work in a corporate setting and

outstanding graduates will become members of the Strategic Support Force, a wing of the People's Liberation Army that is in charge of electronic and cyber warfare. Such collaboration with Chinese universities demonstrates the extent to which China has begun to expand its cyber capabilities. The training in the universities exhibits the enhancements of China's identification, recruitment, and establishment of numerous highly skilled individuals with cyber proficiencies who will then work in the cyber and technology division of China's military force (Yang, 2017).

As technologies such as cloud-based computer networks and IoT (Internet of Things) and various devices and systems connected to the Internet expand, China seeks to steal technological innovations from other advanced countries, such as the United States, to utilize for their own benefits. Various U.S. entities such as sectors focusing on artificial intelligence, Internet connected devices, cloud computing, energy, biotechnology, high-end medical devices and more were targeted in 2017 and 2018 by hackers believed to be linked to China. They have also been continuously accused of hacking companies involved in industrial manufacturing, aerospace, healthcare, solar, and electronics. It is important to consider what companies or government facilities may have also been hacked by China, but went unnoticed and undetected as a result of their advanced proficiencies (Harrell, 2018).

A recent cyber-attack on the Marriott hotel chain is believed to have been enabled by China's intelligence as the U.S. identified computer patterns and codes from the hack that are typically associated with Chinese cyber operations. The attack was performed in order to gather personal information on millions of Americans, namely government and military personnel, as the Marriott hotel is the top hotel where law enforcement and military officials stay. The attack resulted in the Chinese being able to retrieve security clearance files of several Americans. Security clearances tend to contain birth dates, phone numbers, financial data, family

information, and itineraries such as meetings with foreigners. Additionally, Marriott databases do not only contain credit card information, but passport data as well. It was estimated that approximately 327 million consumers were impacted as a result of Chinese hackers stealing their passport numbers. U.S. intelligence reports reveal China's plans and efforts to obtain names of American government officials and executives with security clearances and build a database with such information (Sanger, Perlroth, Thursh, & Rappeport, 2018).

Additionally, one of the most damaging breaches of security for the United States government occurred when China hacked the Office of Personnel Management (OPM) in 2014, acquiring approximately 23 million records of American federal workers. The OPM is the main source for federal government personnel records which include sensitive information. Financial data, social security numbers, and documents containing personal information about those who apply for security clearances are included in the records. Similar to the attack on the Marriott Hotel, Chinese hackers were also able to retrieve information on relatives of those who apply for security clearances. Initiating a two-part attack, Chinese actors disguised themselves as employees of a subcontractor group, KeyPoint Government Solutions, and installed malware, compromising OPM's records (Gertz, 2019). While the attack on the OPM took place in 2014, it was not discovered until 2015. Gathering and aggregating personal data, especially of American government personnel, is a major concern for the safety and security of the U.S. China's ability to access and obtain this personal information leaves the U.S. vulnerable to further threats as China has the advantage of retaining that information to potentially leverage policy or decisions impacting the U.S. (Sanger et al., 2018).

China's global influence. China's recognition of the expansion of the cyber world and its influence has led them to develop approximately a five-year plan involving cyber

enhancements that began back in 2016. The primary function of the plan is to develop cyber innovations in China as well as expand their cyber influence globally. In order to accomplish this, the Chinese are focusing on certain cyber and technological developments such as quantum computing, robotics, semiconductors, and artificial intelligence (AI). Developing, expanding, and improving such technologies will significantly enhance China's influence over the global market as well as give them power in the cyber realm (Segal, 2018).

Unlike most computers, quantum computing gives the computers the ability to perform several calculations at once. Combining technology and mathematics, quantum computing enables a significant increase in the rate at which a problem may be solved. Not only would developments and advancements in quantum computing result in potential economic benefits, but Chinese intelligence may be able to break through current, modern encryptions (Segal, 2018).

Additionally, the Chinese seek to develop artificial intelligence for military purposes with a focus on autonomous drone swarms and software programs to defend against cyberattacks. In order to determine what AI capabilities to develop research on, the Chinese government has studied what AI companies contain the most advanced systems. These companies include Alibaba, the e-commerce company, and iFLYTEK, a voice recognition software establishment. The organizations are among the first to develop superior systems that can drive autonomous cars, act as intelligent voice assistants, and manage smart cities. Learning from these companies who have developed some of the greatest AI capabilities today will help China to determine how to further enhance such developments and excel in AI proficiencies, giving China a greater advantage over cyber global influence (Segal, 2018).

Social media. In addition to technological advancements, social media and its prevalence

around the world significantly contributes to China's global influence. More people in China currently have access to the Internet than any other country (Segal, 2018). Their abilities to access, view, and utilize the Internet allow China to use social media as a means to obtain social and political instability, assisting in carrying out movements and protests that the Chinese government seeks to trigger. Social media remains as a source for information dissemination that aids the government in furthering their political and social agendas. By monitoring social media accounts and sites, they can continue to influence the spread of political or social unrest. The easy access to the Internet, the constant utilization of social media, and the rapid spread of information makes social media a significant platform for influencing political and social change (Jinghua, 2019). China is even working to develop ways to use artificial intelligence for programs that gain access to social media to predict political movements (Segal, 2018).

Solutions. In order to protect companies and agencies from cyber intrusions, the Department of Homeland Security strongly encourages the private sector to take defense precautions. While cyber precautionary measures are beneficial and companies should protect their information and consumers from cyberattacks, it is important to focus on analyzing the scope of cyber threats and identifying those behind them. The Department of Homeland Security has sought to enhance public-private partnerships, as well as develop new technologies, that will improve practices in cybersecurity. Collaboration efforts can be enhanced by gathering information on cyber threats from the public sector and leveraging resources from the private sector. Combined, such partnerships will contribute to identifying, mitigating, and preventing cyberattacks from China (Harrell, 2018).

Intelligence gathering. Local law enforcement officials are often the first to detect a potential threat to the community as well as the first to respond to it. Due to their situational

awareness, it is crucial to enforce efficient and effective information gathering techniques to recognize signs of cyber intrusions early on as well as develop actionable intelligence to influence response efforts and further prevent the threat. In order for local law enforcement to recognize cyber warnings, mitigate impacts, and stop future attacks, they must collaborate with the federal government, the private sector, and the intelligence community.

While cyber threats must first originate in a locality, thereby making local law enforcement the first to respond to the incident, the federal government is crucial in providing resources and developing intelligence to assist in cyber investigations. In order to combat cybercrimes, the Federal Bureau of Investigation (FBI), in particular, has taken several steps to ensure accurate intelligence, improve technological skills, and build partnerships to share developing cyber information (FBI, n.d.).

The FBI has developed a cyber division at their Headquarters and has trained cyber squads with enhanced cyber skills that will assist in investigating various cybercrimes, including theft of personal information and intellectual property and online fraud. The FBI also has Cyber Action Teams that consist of cyber experts that travel worldwide to assist in gathering intelligence regarding computer intrusion cases that are particularly threatening to the security of the United States. The teams contain both agents and computer experts who are trained in forensic investigations, malware analysis, and computer language. Growing partnerships allow the FBI to leverage resources from other federal agencies as well as local and state law enforcement personnel that exhibit situational awareness and retrieve initial information regarding an incident (FBI, n.d.).

Currently, the FBI's Cyber Initiative and Resource Fusion Unit (CIRFU) collaborates with the National Cyber Forensics and Training Alliance (NCFTA) in order to gather

intelligence to combat cybercrimes. The National Cyber Forensics and Training Alliance is a forward thinking organization that proactively addresses cybercrimes by coordinating with law enforcement, the private sector, and academia sources. By collaborating with this organization, the Cyber Initiative and Resource Fusion Unit is able to draw extensive intelligence on cyber related threats that stem from sources such as the private sector, the FBI's Crime Complaint Center, and even the Computer Emergency Response Team from Carnegie Mellon University. Building such partnerships and establishing intelligence sources allows both the FBI's CIRFU and NCFTA to build strategic and tactical products, as well as threat intelligence analysis, to identify and prevent emerging cyber threats (FBI, n.d.).

In addition to the federal government, private sectors have begun to recognize the importance of building alliances to prevent evolving cyber threats. In order to access real time threat intelligence to ensure rapid response efforts, cyber security companies have come together to form the Cyber Threat Alliance (CTA). Organizations such as Fortinet, McAfee, Symantec, and Cisco have developed the alliance to gather intelligence from multiple sources and enhance real time response efforts. The alliance focuses on reducing the time to detect a threat, closing gaps between the detection and deployment cycle, and developing real time cyber threat information sharing among companies in the cybersecurity field. Not only does such information help to prevent cyber attacks more rapidly, but sharing the information among the companies helps to forewarn one another about potential attacks on their systems so that they can immediately respond (Xie, 2018).

The aforementioned companies begin their intelligence gathering by establishing a list of manufactures, OS versions, and devices to determine what devices and systems may be susceptible to exploits and cyber intrusions. After tracking their devices, the companies collect

and analyze data such as IoT and multi-cloud devices to develop threat intelligence. They also work to constantly update logs to ensure that local data is combined with external intelligence needed to gain a full picture of potential cyber threats. Combining data helps to identify indicators of cyber vulnerabilities that require speedy response (Xie, 2018).

Fusion centers. Fusion centers maintain situational awareness, gather information to develop timely and accurate intelligence on impending threats, and share intelligence with appropriate partners such as law enforcement officials and the private sector. The aforementioned abilities allow fusion centers to effectively detect potential threats so that law enforcement can investigate and work to prevent it. Such actions are particularly useful to cybercrimes as detecting a cyber-attack in its early stages is crucial to preventing further damage such as loss of information or stealing of classified, sensitive data (DOJ, 2015).

Integrating the cyber community into fusion centers is extremely valuable in enhancing information gathering and sharing abilities among the centers to combat cyberwarfare of all kinds. Fusion centers are a valuable asset in cybersecurity in that they are a common source for gathering information, such as cybercrime incidents, from multiple partners. Gathering and analyzing such information allows the centers to establish patterns or trends from the data that they can then share with law enforcement and the cyber community. Cyber communities provide fusion centers with information regarding malicious indicators and possible precursors of illegal cyber activity. Such information can include potential patterns of malicious activity, Internet Protocol (IP) addresses, and information developed on new cyber techniques impacting the private sector. They also assist in providing an understanding of raw information such as malware code and abnormal computer activity (DOJ, 2015).

Some fusion centers host cyber community liaisons as resources to efficient information

gathering and sharing capabilities. These personnel tend to exhibit expertise in areas regarding industrial control systems and emerging technologies and software systems. They are also contacts for resources involving cyber subsectors such as Website hosting companies, Internet Service Providers, and mobile platform companies. Fusion centers, in turn, develop relevant cyber products including technical, strategic, and tactical developments, that not only assist in the cyber community but also law enforcement. Sharing pertinent cyber intelligence allows local law enforcement personnel to better prepare for potential threats, such as increased cyber threats from China, as analysis completed by the centers gives law enforcement partners the ability to plan accordingly (DOJ, 2015). As China continues to support Chinese actors committing cybercrimes impacting United States' facilities, integration and collaboration among local fusion centers and local law enforcement is crucial.

In December 2018, two Chinese actors were indicted for conspiracy to commit wire fraud, computer intrusion, and aggravated identity theft. The men, Zhu Hua and Zhang Shilong, are members of the Advanced Persistent Threat 10, or APT 10, a hacking group associated to the Chinese government. By engaging in spear phishing, the hackers were able to introduce malware into targeted computers and subsequently obtain information from said computers. By sending emails that appear to be legitimate, the hackers unleashed attachments that installed a program to record all keystrokes on the machine, allowing them to obtain usernames and passwords. APT 10 has conducted several secretive operations where they were able to steal data from numerous companies encompassing industries such as finance, manufacturing, and health care (FBI, 2018).

The Chinese actors' abilities to not only commit cyber espionage, but cybercrimes such as fraud and identity theft that impact industries in the U.S., require immediate action from local fusion centers and local law enforcement to mitigate such crimes. Similar to their tactics for

espionage, the Chinese engage in online fraud and identity theft crimes by hacking into computer systems, infecting emails through spear phishing, enabling proxies, and influencing social media. The Chinese actors' ability to retrieve classified personal data also allows them to utilize such information to craft spear phishing emails and gain access to any computer. They can similarly use the accounts to send fake emails claiming to be from colleagues in different facilities (Nakashima, 2015). Spear phishing emails affect local businesses, banks, and schools, thus requiring the response of local law enforcement and fusion centers. They are the first to respond and the first to initiate an investigation into the cyber related crime affecting their community.

Limitations / Problems

Based on prior cyber incidents committed by China, as well as continuous advancements in technology and intelligence capabilities, it is evident that China is a threat to the United States and its intelligence community. Although fusion centers can assist in overcoming cyber threats by enhancing intelligence gathering and information sharing regarding cyber threats, there are still challenges that they must resolve. While the aforementioned practices contribute to better preparation and response efforts regarding cyber threats emanating from China, there are also some limitations to combating these threats.

Education. Collecting information on cyber threats requires significant knowledge and understanding of cybercrimes. In order for fusion centers and local law enforcement officials to gather information on cybercrimes, they have to possess significant technological skills, understand cyber related terms, and undergo training on how to investigate, analyze, and preserve such data. Recognizing digital footprints and understanding how different cyber threats, such as ransomwares, are delivered is essential. They must also understand phishing and spoofing terms in order to identify various cyber fraud crimes as well as recognize emails with

potential malware imbedded in them. A lack of education on the part of law enforcement also makes it challenging for the private sector to understand the criminal threat. With a continuous rise in cybercrimes, law enforcement officials must be able to analyze cyber threats and assess their risks, allowing them to provide such information to the private sector (Gercke, 2012).

Jurisdictions. Different regional differences cause some concerns for combating cybercrimes. Not only do different jurisdictions make it difficult to prosecute hackers, provided that they are identified and apprehended in the first place, but it is difficult to coordinate with other countries regarding cyber threats. In order to successfully prevent China from cyber espionage or attacks, the United States must cooperate with other countries who are allies and will aid the U.S. in developing precautions to stop China from committing online crimes. The United States cannot gather all the necessary information and intelligence that is needed to combat cybercrimes originating from China unless aided and supported by other nations (Gercke, 2012).

Funding. These aforementioned developments require funding, education, advanced technologies, and strategic planning and policy developments. In 2017, focusing on the issue of encryption, the Department of Justice requested $21.6 million from the federal budget. The Department of Justice requested the funds in order to acquire new, advanced tools for analyzing encrypted electronic devices as well as develop and expand various in-house expertise. Funding required for cybersecurity appears to be continuously increasing. Further additions such as advanced education and training only add to those costs and create a rather heavy burden on the economy. Even agencies that are well funded may find challenges in acquiring the necessary budget to allot for hiring technology experts, training officers in cybercrimes and updated software systems, and developing and implementing cybercrime prevention policies and

regulations. Rapidly evolving cyber threats make it extremely challenging for the U.S. economy to keep up and continue to ensure cybersecurity (Police Executive Research Forum, 2018).

Conclusion

The staggering change and developments in the cyber world have caused the need for the United States to recognize new cyber-related threats impacting society. As the use of the Internet grows and expands, so do the crimes that take place in cyberspace. The easy access and availability, as well as anonymity, behind the Internet allows hackers, terrorists, and different nation states to take advantage of the cyber realm. Such abilities have created a significant shift from physical crimes to cybercrimes that are predominantly difficult to detect, trace, investigate, and respond to.

China, in particular, has utilized the expansion of the Internet to their benefit. Already involved in numerous espionage incidents in the United States from past events, China has sought to develop their cyber abilities to improve their spying opportunities on the United States. While China tends to focus on private sector companies and stealing their new ideas related to superior technologies, there is also the concern that China is building such capabilities to secure a strong military as well as steal personal data on Americans and intelligence from the American government.

As China continues their developments, it is crucial for the United States to foster intelligence gathering and information sharing among law enforcement partners and the private sector. The private sector is often impacted from such cyber incidents attacking their critical infrastructure and companies' innovations. Law enforcement has the ability to provide knowledge on the cyber threat and investigate. Combining these efforts is crucial to preventing major cyber-attacks. Advanced intelligence gathering and sharing to prevent the attacks can be

developed through the use of fusion centers as they provide situational awareness, develop timely and accurate intelligence, and share cyber related threats among law enforcement personnel and the private sector. Combining resources and efforts among fusion centers to combat cybercrimes will assist in better identifying, mitigating, and preventing cyber threats from China impacting the United States.

The next chapter, Chapter 9, will address technology and critical infrastructure protection. It will specifically focus on the relevance of the information technology sector and its relation to local fusion centers as well as the importance of protecting the sector from criminal and terrorist threats. Chapter 9 will also offer ways to enhance security for the sector and reduce risks.

Chapter 9: Technology and Critical Infrastructure Protection

Introduction

Critical infrastructure includes various assets, networks, and systems that provide for everyday functions and activities of the United States. The critical infrastructure sectors are considered so vital to the operations of the United States that a negative impact on any one of them would have a devastating effect on the safety of the people and security of America (DHS, 2018a). Because the sectors affect essential operations and functions provided by the United States, they also impact fusion centers and their abilities to detect and prevent threats. In order to ensure fusion centers can perform their daily functions, it is essential to protect critical infrastructure sectors that fusion centers rely upon to operate.

Critical Infrastructure Sectors

There are a total of 16 critical infrastructure sectors. The sectors include chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials, and waste, transportation systems, and water and wastewater systems. These sectors are essential to the national security, national public health and safety, and national economic security of the United States (DHS, 2018a).

While all critical infrastructures are vital for the safety and security of the country, the information technology (IT) sector is a rather significant infrastructure in today's society as numerous businesses, companies, government facilities, and citizens rely greatly on the sector. The information technology sector provides both hardware and software services and, along with the communications sector, produces the Internet. Without successful functionality of the sector,

numerous facilities and their operations may fail, thus affecting the economy. Without the infrastructure, a lack of daily communications that citizens rely on through Wi-Fi and the Internet may lead to panic. Most importantly, government facilities that operate under advanced information technology systems may be compromised, thus threatening security and safety of the public (DHS, 2017b).

While impacted by several critical infrastructure sectors such as communications and energy, local fusion centers and their operations rely greatly on the information technology sector and are directly impacted by its functions. Through computers and other hardware products, fusion centers utilize software systems and databases to gather, store, retrieve, and share information (DOJ, 2009). As a result, in order for fusion centers to effectively gather and share such information, the information technology infrastructure must be protected and defended from any threats that could compromise or destroy its functions and capabilities.

Information technology assets. In order for the information technology critical infrastructure to remain secure, it is important to protect its critical nodes and links. Critical nodes are the sector's most valuable assets that if compromised or threatened in any way could severely harm the overall operations and functions of the sector. In addition to the critical nodes, the critical links demonstrate the connection between the assets. In some sectors, it would require several assets to be negatively impacted in order for the sector to drastically be affected. In others, however, the threat or negative impact on just one critical node could have severe repercussions on the sector (Dhurde & Deshpande, 2014).

Hardware products and software systems. Hardware products and software systems are the critical nodes of the IT sector as they allow the sector to perform its operations. Hardware products consist of items such as computers, ipads, smartphones, hard drives, routers, firewall

hardware, and more. Such items are essential to the information technology sector as they are the physical products that allow access to software systems, databases, and the Internet. Software systems, on the other hand, include operating and application systems that provide the ability to perform certain, specific tasks. Examples of software systems include Microsoft Office and Internet browsers such as Safari and Google Chrome. Additionally, the software systems allow for the creation of databases that gather, store, retrieve, and share information (IT Infrastructure, 2013).

Both the hardware products and software systems of the information technology sector greatly rely on one another. The negative impact on one asset has the potential to affect the other asset and cause a significant failure to the sector. Without the hardware products such as computers and ipads, there would be no way to access the software systems, databases, or the Internet. Similarly, without access to the software systems and databases to collect, retrieve, or share information, the hardware products would remain useless. Both critical nodes must be protected to ensure that information technology remains secure and that a catastrophic failure does not occur (IT Infrastructure, 2013).

Information technology threats. Because the information technology sector supports the United States' every day functions, it is vital to ensure that the critical nodes of the information technology sector are protected against threats. Some threats include both cyber and physical attacks. Cyber-attacks include any harmful act conducted in cyber space in the attempt to dismantle or destroy a computer system or network. Cyber-attacks are particularly threatening to the information technology sector as the critical infrastructure relies almost solely on the Internet and computer systems to perform their everyday activities. A cyber-attack on the sector

would severely impact its software systems, and databases, thus impacting the entire sector's functions (Fisher, 2016).

Cyber-attacks. Cyber-attacks are often performed by hackers with the intent of either stealing, distributing, or destroying classified information. Because fusion centers often gather and share vital, classified intelligence, an attack on their software systems would cause a breach in security. Similarly, years of intelligence from wide-scale operations could be compromised or potentially destroyed from a cyber-attack. Such attacks even have the potential to be deployed by internal threats, whereby individuals already have the skills, due to training, to complete cyber-attacks. In addition to hackers, terrorists may have an interest in attacking through cyberspace. A negative impact on the Internet or Wi-Fi would result in people not being able to communicate with one another. Additionally, companies and facilities that operate through technological systems would shut down and be negatively impacted economically (Fisher, 2016). Such repercussions can result in public fear and panic.

Physical attacks. In addition to cyber-attacks, physical attacks may also take place. Physical attacks will often harm the hardware products in fusion centers that allow for the utilization of software systems and databases. Such instances can stem from terrorism, through the physical attacks of companies or government facilities that host numerous hardware services in their buildings, thus destroying them. The attacks may also stem from natural disasters that cause damage and destruction to homes, businesses, institutions, and many more that operate with hardware products. Just as with software systems, any drastic impact on the hardware products alone could cause damage to the entire IT sector (IT Infrastructure, 2013).

Although both cyber and physical attacks have the potential to develop serious consequences for the operations of the information technology sector, cyber-attacks have a much

greater probability of occurring than physical attacks. Cyber-attacks are often successfully accomplished because of the level of advancements that society has reached in regard to the cyber world. Hackers can now hack systems at an accelerated speed and break through firewalls seamlessly and without detection. In addition, terrorists can utilize IT to their benefits by reaching out to young, impressionable individuals for recruitment through social media. Such easy access to the online world has not only made gathering supporters significantly easier for terrorists, but it has allowed them to spread their ideologies all over the world. Lastly, cyber-attacks can be accomplished quickly and quietly. In some instances, companies, institutions, or government facilities will not know that they have been hacked or compromised until it is too late and their systems have been breached (Weimann, 2004). Such stealthily operations are particularly concerning for the IT sector and fusion centers.

Risk-Based Resource Allocation

In order to disrupt threats to the information technology infrastructure, countermeasures to protect the sector must be developed. Such countermeasures can be developed through the apportioned risk reduction method. The apportioned risk reduction includes spreading available resources and funds across as many threats to the sector as possible. This, in turn, helps to reduce the risk to all potential threats to the sector (Lewis, 2006).

Security measures. In order to protect the sector, security measures should be checked on, as well as advanced, constantly and consistently. Security systems must be monitored at all times to ensure that they are functioning and that they have not been compromised. They should also be updated often. If the security systems remain the same, it becomes easier for the attackers to recognize the current system and locate potential weak spots where they can penetrate the system. Constantly monitoring and building security efficiency and performance helps to avoid

complacency, which would otherwise make it extremely easy for attackers to initiate their plans and successfully attack. Similarly, updating and reviewing emergency plans, should an attack take place, will help to build procedures to fix current security flaws (Vulnerability Assessment, 2001).

Training. It is also important to retain personnel that are highly advanced in technology and cyber skills. Not only should their skills be proficient, but they must be able to recognize threats early on. Whether it be a virus spreading throughout the networks or hackers stealing classified information, it is essential that the IT security personnel recognize warning signs early on. If the attack cannot be prevented, then at least early recognition will ensure that there is not complete destruction or loss of information or intelligence. They should also be able to recognize emails or links that may contain viruses that are harmful to their servers. Such superior skills can be developed through advanced training programs that focus on topics such as hacking, viruses, failure of software systems, as well as ways to prevent and respond to such incidents. The programs should essentially develop experts in the evolving information technology sector where the personnel supporting United States government facilities can begin to surpass the skills of hackers (Vulnerability Assessment, 2001).

Information sharing. Lastly, it is essential to forewarn other centers and agencies should a cyber-attack take place, especially in local fusion centers. If fusion centers are able to recognize the initial stages of a cyber-attack in their center, they must caution other agencies about a potential attack on their systems. The centers gather and develop their intelligence by sharing information with other centers and agencies. They also share several databases where the information is stored and shared (DHS, 2017c). Should the information in one center be compromised by a cyber-attack, then other centers may be impacted as well. Collaborating with

other fusion centers to prepare for and prevent cyber-attacks will assist in disrupting further damage to the centers and protect important, classified information that each has gathered and shared over periods of time.

Redundancies. In the event that a cyber-attack does take place, response plans must be in place. If fusion centers fall victim to a cyber-attack, the centers must look towards their federal partners to provide them with the necessary resources and funds to restore their operations as quickly as possible (DHS, 2017c). Additionally, the center must collaborate with the Multi-State Information Sharing and Analysis Center (MS-ISAC). MS-ISAC is a facility designed as a key resource for cyber threat prevention, response, and recovery for the country's local, state, tribal, and territorial partners. Designated as a cyber-resource by DHS, the facility serves local fusion centers and can greatly assist in response efforts in the event of a cyber-attack. Composed of security experts, the center's Computer Emergency Response Team (CERT) also provides malware analysis, malicious code analysis and mitigation, computer and network forensics, and incident response. Fusion centers can report incidents ranging from unauthorized access to intelligence, compromised passwords, execution of viruses or malware, and more. CERT responds with forensic analysis, reverse engineering, threat intelligence, and mitigation and response efforts (Multi-State Information Sharing & Analysis Center, n.d.).

Budget. Protection for hardware products and software systems in fusion centers requires sufficient funding and grants from the Department of Homeland Security. Specifically, the centers are often funded by the Homeland Security Grant Program (HSGP) that helps to ensure equipment for core capabilities for operations and security for the facilities. The program consists of the State Homeland Security Program, the Urban Area Security Initiative, and Operation Stonegarden. Combined, these programs fund the necessary equipment that fusion

centers request in order to strengthen their abilities and their overall missions (DHS, 2018c).

In order for fusion centers to request funds for their hardware products and software system, they must comply with several rules. The requests regarding the investments should reference the specific performance areas that the funding is intended to support or reasons why the funding is requested and deemed necessary for the centers. Additionally, all centers in different jurisdictions should be able to utilize the requested funds. The funds should support various centers and their activities in intelligence gathering and sharing. Local fusion centers seeking the funds must ensure that efforts in support of the centers' initiatives are integrated and coordinated with other fusion centers (DHS, 2018c).

Fiscal year. Accompanying the fiscal year 2018 Appropriation for the Department of Homeland Security, Congress expressed that the Secretary must fund up to 85 percent of the nationwide risk. As a result, the Secretary designated 32 urban areas that were eligible for such funds under the Urban Area Security Initiative. One of the facilities eligible for the funds included fusion centers as Congress found it necessary to utilize the funds for the centers in order to prioritize cybersecurity projects and technological integration and capabilities to assist in managing emerging threats (DHS, n.d.).

While several other groups and facilities were allotted funds from the Urban Area Security Initiative (UASI), overall the program received approximately $580,000,000 in 2018 to share with each group and put towards their efforts (FEMA, 2018). Depending on how much of the funds the other recipients of the program require for their initiatives, fusion centers have the ability to utilize the allotted budget from the Initiative to support their technological advancements and security systems for their operations (DHS, n.d.).

The allotted budget for the centers must be split to support both the hardware products

and the software systems. As previously mentioned, the apportioned risk reduction takes the given budget and spreads it evenly among the critical nodes of the infrastructure in order to protect the sector's assets and reduce the risks to all possible threats (Lewis, 2006). The budget can be used for costs of new computer systems or additional iPad as well as advanced software systems and anti-virus and anti-malware systems for the centers. Databases can be expanded to store vast amounts of information and technological advancements can be made to ensure that systems are interoperable among various agencies. Backup systems may also be developed and implemented in the event of an attack. Lastly, the budget can assist in training purposes so that analysts and law enforcement individuals who work in fusion centers are trained in advanced information technology systems. While the budget may fluctuate from year to year, the goal is to show the importance of fusion centers and the functions of their IT critical nodes so that they can receive the highest budget possible to continue to advance their systems to defend against any cyber-attacks (DHS, n.d.).

Conclusion

In order to protect and secure the information technology sector, it is necessary to protect its hardware products and software systems as harm to these assets could have potential dire consequences to the sector and its functions (IT Infrastructure, 2013). This is particularly true for fusion centers that operate through software systems and databases to store, retrieve, and share vital information. Based on the centers' use of technology, software systems, and databases, there is a high probability that threats will emanate from cyber-attacks, rather than physical. As a result, it is important to strengthen security measures, retain personnel that are highly advanced in technology and cyber skills, and forewarn other centers and agencies should a cyber-attack begin to take place.

Chapter 10 will discuss the benefits of multidisciplinary approaches to homeland security. More specifically, it will address how fusion centers can also assist in all hazards by collaborating and coordinating with several different disciplines.

Chapter 10: Multidisciplinary Approaches to Homeland Security

Introduction

In order to enhance collaborative efforts of fusion centers, it is vital to adopt multidisciplinary approaches. Multidisciplinary approaches include integrating numerous disciplines into a collective community to build successful homeland security plans (Wyckoff, 2015). While fusion centers often collaborate with law enforcement personnel, they should also cooperate with varying disciplines in emergency management. Although fusion centers primarily assist in criminal and terrorism-related incidents, their abilities to function as a conduit for information sharing may prove to be beneficial for all types of hazards (Harris, 2008).

While disciplines such as police, fire, emergency management personnel, health providers, etc. often maintain different resources, roles, and responsibilities, they share similar goals in seeking to prepare for, mitigate, and prevent manmade events and natural disasters. Because several disciplines become involved in emergencies, fusion centers can assist in emergency management by sharing information with responders. In order to do so, fusion centers and the various disciplines must come together to strengthen collaborative efforts.

Emergency Preparedness and Response

The emergency management cycle can guide fusion centers and various disciplines to build collaborative plans and practices for emergency management. The emergency management cycle contains essential activities that all partners must follow in order to prepare for and respond to an incident. More specifically, the cycle is comprised of planning, organizing, gathering equipment, training, exercising, and evaluating and improving.

Emergency management cycle. Planning involves the collection and analysis of information as well as the development of procedures. It allows the stakeholders to learn their

roles, as well as others, in the plan and determine capability requirements early on. This greatly aids in shortening the time required to gain control of an adverse event. Organizing is the process of strengthening leadership at each level and developing an organizational structure where responders can work together more efficiently. In order to practice the developed plan and perform assigned tasks, it is important to acquire various equipment, supplies, and systems. Analysts, law enforcement personnel assigned to fusion centers, and other disciplines must be able to share commonly understood resources when responding to a severe incident. Training prepares the partners with the training and assets to accomplish their goals. Exercising includes practicing the plans that have been developed. Testing the plans with all partners aids in determining whether they may be successful or not. Lastly, evaluating and improving complete the emergency management cycle. Evaluating strategies helps to identify what is working successfully as well as any deficiencies that may exist in the plans. Whether or not the plan is considered successful, it is important to always continue improving and developing specific recommendations for changes in practices (DHS, 2008).

Whole Community and Mega-Communities Concepts

A whole community consists of different disciplines, such as emergency management personnel, government officials, the private sector, and the public, collectively assessing the needs of their communities to strengthen their capacities (FEMA, 2011). In order to strengthen the communities' capacities, the whole community can build a megacommunity and collaborate together. Megacommunities include various disciplines, such as law enforcement, fire, medical services, public health, emergency management, and leaders within them, coming together to work towards common goals (DHS, 2008). Megacommunities also acknowledge the importance of incorporating businesses, government, and civil society in the relationship. Developing such

open-ended networks where disciplines can learn from one another, share resources, and develop partnerships is what strengthens their approaches to homeland security strategies. Integrating the disciplines into a megacommunity develops greater emergency management planning, communication pathways, and resilience (Gerencser, Van Lee, Napolitano, & Kelly, 2008).

Fusion centers benefit from forming a megacommunity in that they are able to better collaborate with different partners to gather and share information in a timely manner. Sharing such information in a timely fashion helps to detect threats in an expedited time frame, catch suspects before they commit further crimes, dismantle potential criminal or terrorist operations, and potentially assist in emergencies, such as natural disasters, by providing information to response teams. Additionally, while several disciplines retain different tasks such as gathering and sharing information, caretaking and providing services to victims, or organizing response plans, they all share similar goals in preventing or mitigating adverse incidents. Developing a megacommunity with fusion center personnel and various disciplines allows the groups to better collaborate as a team.

Partnerships. Fostering partnerships among the different disciplines helps to increase collaborative efforts among fusion centers. Partnerships assist in strengthening cooperation among the disciplines to improve preparedness and response methods. While each discipline often maintains their own roles, tasks, and resources, they all tend to have a level of dependency on one another. Without cooperation among them, it would be extremely difficult to ensure the best possible results for otherwise adverse events.

Fusion centers coordinate with various partners, including local, state, tribal, and federal levels through the receipt, analysis, gathering, and sharing of threat-related information (DHS, 2017d). In an adverse incident, the local level initiates the response as they maintain situational

awareness in their community. Within the community, local fire, emergency services, public health, police, and several other responders are usually the first to respond to an incident as well as the last to leave the site. Additionally, the state assists the local level in their abilities as they provide resources to them. The tribal level also often requests the states' varying resources and assistance when needed. Federal partners contribute to domestic incidents and regularly maintain several operations by supporting fusion centers and their initiatives. For example, fusion centers often collaborate with local FBI joint terrorism task forces where they can utilize federal government resources and share homeland security information (DHS, 2016). Similarly, fusion centers support the federal government by providing them with critical state and local intelligence and subject matter expertise (DHS, 2018b). Non-governmental facilities also aid in response measures by acquiring local volunteers, providing emergency services such as food and water, and implementing search and rescue (Course Overview, n.d.).

Lastly, the private sector has become a major influence in multidisciplinary approaches, including collaborating with fusion centers. Private sector partners are typically the first to detect precursor criminal or terrorist activity. Developing a strong partnership among the private sector and fusion centers assists both government and industry decision makers in better understanding, detecting, preparing for, and responding to emerging threats while also aiding in reducing risks to the community (DHS, 2014). The private sector also has resources, such as specialized experts and equipment, in varying disciplines that can greatly assist in response and recovery efforts. Private sector partners help to restore infrastructure and they participate in both state and local preparedness activities (Course Overview, n.d.), helping to mitigate repercussions in emergencies.

Partnerships also build trust, making it easier to communicate and work with one another.

Within the Federal Bureau of Investigation, there is an organization called the Office of Private Sector. The Office of Private Sector partners with the FBI in order to develop organized and coordinated approaches to engagement with the private sector. The operations of the office include enhancing the FBI's understanding of the risks and needs of the private sector as well as increasing information sharing between the private sector and the bureau. The overall goal of the office is to mitigate threats through long-lasting, mutually beneficial partnerships between the federal government and the private sector (DOJ, n.d.b).

The office has also developed a group called The Domestic Security Advisory Council. The Domestic Security Advisory Council (DSAC) is an information sharing and security initiative between the FBI, the private sector, and the Department of Homeland Security. DSAC enables effective communication and information sharing in order to investigate threats that impact, specifically, American businesses. The council supports the private sector by advancing their capabilities to protect their assets, infrastructure, employees, and proprietary information. Essentially, the council also helps to bridge the gap that exists between fusion centers and the private sector. Because the FBI often partners with fusion centers, DSAC's inclusion within the FBI gives them some access to information sharing between local fusion centers. It is these types of partnerships that allow for mutually beneficial strategies and outcomes for fusion centers and their abilities to assist in emergencies (DOJ, n.d.a).

Dialogue. One of the best methods to utilize when seeking to build partnerships and encourage multidisciplinary approaches is dialogue. Dialogue is a form of conversation that supports moving past one individual's understanding and perspective to build collective meaning and community. Through collaborative meetings with one another, dialogue should be enforced in fusion centers so that each partner can share and learn different perspectives. The practice of

dialogue allows for new understandings, creative ideas, shared leadership, and a community-based culture of cooperation among the partners collaborating with fusion centers. Dialogue is an effective means of establishing multidisciplinary approaches to homeland security in that it moves the disciplines from their cultures of dependency, competition, and exclusion to increased efforts in collaboration, partnerships, and inclusion. The disciplines can still retain their ability to share their strengths and ideas while allowing others to learn and integrate multiple different perspectives (A Brief Orientation to Dialogue, 2006).

In order to build dialogue in the megacommunity, targeted forums are valuable initiatives that can be particularly beneficial for fusion centers. Targeted forums include large, cross-sector conferences where various personnel come together for several days to discuss and collaborate on a specific topic. This process teaches personnel how to work with one another, thus fostering collective action. It helps them develop contacts for future collaborative projects. It also builds trust among the partners and encourages open discussions for different ideas. Because fusion centers acquire their intelligence through information sharing with different partners, a sense of trust and cooperation are essential qualities that the partners must exude. The partners must be comfortable enough with other disciplines and partners to constantly and consistently reach out and share information. Prolonged meetings, such as the targeted forums, will assist in developing such elements, thus supporting both the fusion centers' objectives and the overall megacommunity (Gerencser et al., 2008).

Leaders. In order to instill a megacommunity, it is essential to ensure that there are leaders with certain attributes that allow the megacommunity to flourish and remain longstanding. Namely, there are ten important key elements to becoming a successful leader in a megacommunity. These ten qualities include a spirit of inclusiveness, tri-sector exposure, a non-

imperial approach, navigation skills, communication skills, technological savvy, adaptability, the talent to foster talent, presence and passion, and long-term thinking (Gerencser et al., 2008).

Inclusiveness not only applies to the megacommunity participants but also to the citizens who stand to benefit from disciplines collaborating to ensure safety and security. A tri-sector exposure is dependent upon a leader having experience in all three sectors including business, government, and civil sectors. Their familiarity with the aforementioned sectors and their responsibilities will assist in integrating the different disciplines into the megacommunity. A non-imperial approach ensures that a leader is not overbearing, but rather supports the groups in their work production. Navigation and communication skills involve creating pathways to strengthening collaboration, inventing strategies that work for all, and listening and speaking to everyone in the process effectively. Technological savvy and adaptability ensure that the leader grows in knowledge as advancements continue and are able to progress from such technological innovations. Leaders must also bring about each sector's talent and continue to encourage their most valuable qualities and capabilities. Additionally, presence and passion will support such talents as the leaders' passion for their responsibilities and the goals they seek to acquire will also encourage the partners involved. Lastly, long term thinking is essential in reaching the megacommunity's goals. It creates sustainability where the partners in the megacommunity begin to become invested in the megacommunity process as well as committed to ensuring that their shared goals in homeland security are accomplished (Gerencser et al., 2008). While it may be difficult to acquire leaders with all of these ten valuable assets, leaders should strive to possess such strong qualities to ensure that they maintain the megacommunity.

Community resilience. One of the valuable qualities of fusion centers is that they have close ties to the community and locality that they are based in, making them extremely beneficial

in supporting community resilience against threats. A resilient community entails an engaged local community, partnerships among different organizations, integration of preparedness and response plans, and partnerships with state and federal government (Chandra et al., 2011). For this reason, it is important that fusion centers sustain a megacommunity as they heavily support other disciplines by allowing them this pathway to information from the local community.

Emerging Security Technologies

As society continues to advance in technology, a common threat that faces the country are cyber threats. These types of threats are particularly concerning for fusion centers since the centers are surrounded by technology as they utilize different hardware products and databases to store, retrieve, and share information (DHS, 2017c). In order to remain ahead of these potential threats, fusion centers collaborate with the cyber community. Often cyber community personnel may be staffed in the centers, acting as analysts or IT liaisons. These personnel remain aware of emerging security technologies that can assist in detecting and preventing threats. Additionally, they have contacts within the federal, state, local, tribal, territorial (FSLTT), and private sector cyber community that act as resources for providing valuable intelligence on cybersecurity and cybercrime as well as the development of advanced hardware, software, and emerging technologies. Cyber personnel also assist in providing detection, mitigation, and recovery activities as they can assist law enforcement personnel with a variety of surveillance and prosecution capabilities. They share risk information on suspicious activity or cyber indicators with fusion centers. Such a partnership with the cyber community allows fusion centers to better prepare for and respond to adverse cyber threats that could otherwise potentially cause numerous security concerns for the country (DOJ, 2015).

Conclusion

Fusion centers rely on collaborating with different partners to gather and share threat-related information (DHS, 2018a). It is through the integration and cooperation between the partners that the centers can share information to detect, mitigate, and prevent manmade incidents. Additionally, the centers have the potential to assist in all hazards and emergency management (Harris, 2008). Coordinating with disciplines such as police, fire, public health, and emergency management allows the centers to become part of a megacommunity that integrates these partners' efforts to prepare for and prevent emergencies. Such collaboration helps to integrate different skills and gather and share information in a timely fashion, thus building community resilience and security of the country.

Chapter 11 will include public health and pandemic issues and their relation to fusion centers. It will address current public health challenges as well as how to prepare for and respond to them.

Chapter 11: Public Health and Pandemic Issues

Introduction

As threats to public health expand, there is a need to better prepare for, respond to, and recover from such incidents. Fusion centers remain in a position where they can assist in such activities by sharing data and collaborating with various public health agencies, law enforcement personnel, and response teams in emergencies. By strengthening fusion centers' efforts to coordinate with public health, they can share data and provide strategic and tactical information that will contribute to mitigating public health incidents such as weapons of mass destruction, explosives, and pandemics.

Scope and Complexities of Public Health Challenges

Public health threats often stem from different sources. Some emanate from terrorist threats through biological, chemical, radiological, and nuclear agents, or explosives. Others stem from naturally occurring incidents such as influenza pandemics. While such health concerns may originate from various sources such as manmade, natural, or accidental, most overlap in that they result in similar challenges and adverse repercussions (U.S. Government Publishing Office, 2008).

Weapons of mass destruction. Weapons of mass destruction, including biological, chemical, radiological, and nuclear agents, remain as one of the greatest risks to the national security of the United States. Such agents in the possession of adversaries, hostile states, or terrorists, have the potential to cause significant damage to the country. An attack utilizing these weapons of mass destruction could result in critical infrastructure failure, economic instability, and mass casualties. Not only do they have the potential to inflict harm in the United States, but they can cause injury to military forces abroad (GPO, 2008).

Explosives. Similar to weapons of mass destruction, explosives may be created and planted by terrorists in an attempt to instill fear and cause mass casualties. Terrorists targeting passenger concentrations at airports by transporting explosives through unsecured air transportation routes remains as a serious threat. The potential of the use of explosives remains high as terrorists often retain the necessary technological skills to make them as well as the ability to obtain the components for improvised explosive devices. In addition to the numerous deaths that can result from the initial blast of explosives, radioactive particles can spread thereafter, impacting even more lives and the health of the public (GPO, 2008).

Pandemics. Unlike terrorist threats, pandemics are naturally-occurring incidents that can negatively affect public health. Pandemics are widespread outbreaks of infectious disease that significantly impact morbidity and mortality rates over a wide geographic area. As time continues, pandemics appear to be increasing in frequency largely due to emerging viral diseases from animals. Greater exploitation of the natural environment and increased global integration and travel contribute to the increase as well. While pandemics can stem from several different diseases, influenza is most likely to cause a massive pandemic and complicate the health of large populations (Madhav et al., 2017). Contagious diseases such as influenza pandemics spread rather easily and rapidly, causing a vast amount of people to be infected and even more to panic and become fearful that they, too, will become infected **(**GPO, 2008).

Challenges. In addition to many hospitals already struggling to manage the volume of patients who require care on a daily basis, the aforementioned emergencies cause greater issues. Public health emergencies tend to result in medical surges and a drastic increase in patients in hospitals needing immediate care. Paramedics often have to wait for extended periods of time before patient care can be transferred to the hospital staff. An overflow of patients and high

occupancy leads to patients being treated in emergency department hallways where they may be held for hours before they can be placed in an inpatient bed. Transferring patients to alternative care sites can be difficult due to the personnel, equipment, and time that is needed to do so. Damage to infrastructure in the event of an emergency may also impede responders' abilities to transfer patients. A lack of disaster preparedness and response education for most medical and nursing school curricula also contributes to the difficulty of ensuring better response efforts to public health emergencies (Department of Health and Human Services, n.d.).

Additionally, maintaining enough resources and personnel in hospitals and public health facilities that can assist in major incidents is a challenge. In the event of an emergency, there are often shortages of supplies and essential equipment as many facilities in a given area use the same suppliers for back-up stock and medical supplies. Hospitals generally face shortages in personnel, but during emergencies such as terrorist attacks or natural disasters, such shortages are only exacerbated. Nurses, doctors, and public health professionals have their own personal family responsibilities that they must attend to in such incidents. They, themselves, may also have been severely impacted or harmed by the adverse event. Others may simply be afraid to respond during a disaster due to personal safety concerns (Department of Health and Human Services, n.d.).

Communication failure is a constant, recurring theme often seen during and immediately after a disaster. Emergency response involves numerous different disciplines including fire, police, public health, emergency management, EMS, and more. These disciplines must be able to collaborate effectively to prevent further injuries and save lives, yet it is challenging to develop a communications system that is interoperable among all public safety disciplines as well as public volunteers. It is also difficult to ensure enough resources, such as radio or satellite phones, for

communication purposes especially if there may be an overflow of personnel assisting in the disaster. Without effective preparedness plans that incorporate clear roles and responsibilities among public health professionals, public safety personnel, and volunteers, it is nearly impossible to mitigate an emergency (Department of Health and Human Services, n.d.). For example, a lack of preparedness for the wide-scale attack of 9/11, impeded effective decision-making from command structures. Lack of effective preparedness for the magnitude of the incident, number of responders needed, and plans to collaborate with countless public safety personnel hampered some response efforts. Senior leaders could not reach other officials and some did not enter the chain of command until after the morning's attacks due to the inability to efficiently communicate (Summary of Final Report, 2014).

In order to ensure effective communication and efficient response efforts among different public safety disciplines, emergency departments support numerous responsibilities. The emergency department in hospitals is the primary site were initial information regarding a disaster is communicated. The emergency department is there to determine the extent of the disaster so that they can ascertain how best to respond to it. The department is responsible for handling various, different disasters and making timely and accurate response decisions such as initiating an institutional lockdown, determining if recipient victim decontamination is needed, and declaring an institutional disaster. Their abilities to retrieve initial information, make decisions regarding response procedures, and share the information with the regional emergency operations center and hospitals are crucial to mitigating an emergency (Department of Health and Human Services, n.d.).

Fusion centers. Much like the roles of emergency departments involving information gathering and decision making, fusion centers also support information gathering and sharing. As

threats regarding public health emanate, the importance of intelligence and sharing such information becomes crucial in better preparing for and responding to such adverse incidents. Due to their unique situational awareness, fusion centers can assist public health officials in identifying, mitigating, and preventing various threats to public health (Barishansky & Komansky, 2014).

Fusion centers have begun to expand their capabilities to an all-hazards approach with a focus on developing partnerships with various disciplines. Public health officials can offer fusion centers strategic and tactical information such as crime-related trends, response capabilities, and suspicious activities related to health. Local and state public health officials often provide public health intelligence such as communicable disease trends, environmental health findings, surveillance observations of critical symptoms, and private healthcare-capacity such as medical surges. In return, fusion centers develop analytic products outlining potential causes for concern that they may identify from such information, utilize their surveillance capabilities, and use their detection tools to better collaborate with different disciplines including homeland security and first responder partners. Fusion centers have the ability to recognize patterns, detect connections, and develop accurate intelligence. They can bring together expertise from distinct areas of the emergency services community to ensure timely and efficient preparedness, response, and recovery efforts to various health threats (Barishansky & Komansky, 2014).

Policy, Strategic, and Ethical Issues Related to Preparedness and Response

Public health concerns including weapons of mass destruction, explosives, and pandemics are not considered new threats as these threats have previously impacted the United States. Past incidents have greatly compromised the health of the public while also causing significant building damage, economic loss, and mass casualties.

Weapons of mass destruction. In 2001, B. anthracis spores, also known as anthrax, were sent through the United States postal system in a bioterrorist attack. A public health investigation was first implemented when an infectious disease physician recognized a potential case of inhalation anthrax in a patient hospitalized in Florida. The diagnosis was soon confirmed by Florida's Department of Health (FDH) as well as the Centers for Disease Control and Prevention (CDC). As the investigation continued, various victims of possible anthrax exposure turned up in different areas of the country including Manhattan and New Jersey. Symptoms of inhalational anthrax in New Jersey postal workers appeared and the workers were subsequently diagnosed with anthrax exposure. Another individual staffed in the Hart Senate Office Building opened a letter that contained a powder substance along with a note identifying the substance as anthrax. Nasal swab tests were performed on hundreds of senate staff members and visitors to the building, resulting in 28 victims being exposed to anthrax. Through further investigation and analysis, the CDC was able to link four confirmed cases of anthrax as a result of intentional delivery through mailed letters or packages. The 2001 anthrax attack resulted in 22 people developing anthrax due to the mailings, 11 suffering from the inhalational of the substance, and 5 of them dying (Gursky, Inglesby, & O'Toole, 2003).

Explosives. Leading up to 9/11, there were several attacks by terrorists seeking to eliminate numerous Americans and cause severe destruction. In February of 1993, a terrorist group, led my Ramzi Yousef, attempted to bring down the World Trade Center with a truck bomb resulting in 6 deaths and a thousand wounded. Terrorists' bombings and threats on Americans have also occurred outside of the U.S. In November of 1995, five Americans were killed in a car bomb explosion that occurred outside the office of the United States program manager for the Saudi National Guard in Riyadh. A truck bomb killed 19 United States

servicemen in Dhahran, Saudi Arabia in 1996. Additionally, bombings of U.S. embassies in Kenya and Tanzania occurred in 1998 and two years later, an al Qaeda team planted explosives in a motorboat in order to blow a hole in the side of a U.S. destroyer, killing 17 American sailors (Summary of Final Report, 2014).

Pandemics. The pandemic spread of influenza viruses is typically characterized by a high attack rate and an increased level of mortality, namely in young adults. A rather prominent pandemic is the 2009 Swine Flu (H1N1) pandemic. Classified as Influenza A H1N1, this new strain of Influenza A virus caused a major outbreak of human infection in the USA and Mexico in April of 2009. The virus is typically transmitted by respiratory droplets and can be spread by the touch of hands. This particular strain has a higher level of transmissibility than other seasonal influenza strains. Throughout the 2009 pandemic, many people who were infected experienced fevers, cough, sore throat, fatigue, shortness of breath, headache, vomiting, and various other symptoms. For those who already had medical complications such as chronic respiratory diseases, immune suppression, neurological disorders, diabetes and obesity, however, they experienced additional symptoms including pneumonia and peripheral neuropathy. The first cases of influenza A H1N1 pandemic were identified in April of 2009 in the U.S. By August of 2009, approximately one million people were infected in the U.S. alone (Al-Muharrmi, 2010).

Preparedness and response efforts. These aforementioned incidents involving weapons of mass destruction, explosives, and pandemics lead to severe repercussions on society and public health. As advancements are made and the threats become greater, it is even more crucial to ensure that there are efficient and effective preparedness and response efforts to combat these growing threats.

Weapons of mass destruction. Diplomacy, threat reduction assistance, and export

controls are all measures that must be taken in order to prepare for threats involving weapons of mass destruction. Such measures assist in impeding other states and terrorist organizations from using such weapons to cause severe damage to the U.S. They also help to slow down their ability to obtain the necessary materials to develop weapons of mass destruction as well as increase their costs to access sensitive technologies and expertise. While it is essential to protect the U.S. from other states and terrorist organizations utilizing weapons of mass destruction on U.S. soil, it is also important to support allies and the international community. Working closely with like-minded countries increases the United States' ability to stop the spread of weapons of mass destruction and develop recycle and fuel treatment technologies that are more efficient, cleaner, and more proliferation-resistant. In order to improve the ability to gather accurate and timely knowledge on adversaries' capabilities regarding these weapons of mass destruction, effective intelligence, surveillance, related technologies, and research on the evolving threats must be reinforced. Particular emphasis should be placed on intelligence collection and analysis on weapons of mass destruction, interaction among U.S. intelligence and law enforcement, and intelligence cooperation with allies (GPO, 2008).

Explosives. Explosives are often acts of terrorism that include any chemical compound mixture, or device, used to detonate a bomb such as improvised explosive devices (IED's). Combatting the use of explosives includes utilizing developing technologies and capabilities to detect, locate, and render the devices safe before they detonate. This includes enhancing training and education efforts for bomb technicians and law enforcement officials to recognize precursor chemicals and materials used to develop improvised explosives or incendiary mixtures. Psychological and behavioral sciences should also be used to analyze potential threats of an explosive attack. Similar to most threats, combatting the use of explosives requires significant

coordination among local, state, tribal, territorial, and federal governments as well as the private sector, including operators and owners of critical infrastructure. Strengthening these partnerships will enhance communication efforts regarding accurate and timely information sharing in the event of a potential attack by means of explosives (GPO, 2008).

Pandemics. Because the spread of a pandemic can lead to massive suffering and potential deaths, negative economic impacts, and mass panic by society, preparing for such incidents is necessary. Preparedness must include means to ensure clear communication of all responsibilities to levels of government, public health officials, and society. This entails educating society about high-risk practices involving potential increases in virus transmissions. It is the responsibility of health and medical officials to disperse information and education regarding epidemic and pandemic illness. Surveillance and detection practices provide situational awareness to ensure early warnings and detection of an outbreak of a disease and possible pandemic. Should a pandemic occur, response and containment plans assist in mitigating the spread of the outbreak as well as social, economic, and health impacts. Vaccines and antivirals are essential countermeasures. There must be a sufficient amount of vaccines available to vaccinate individuals within a certain timeframe of the emergence of the virus as well as plans to prioritize high-risk populations. In addition to ensuring resources such as vaccines, it is important to rapidly recruit and deploy health, medical, and veterinary providers with the necessary skills to assist in these types of emergencies. Their assistance is vital as pandemics will often lead to medical surges that require a vast amount of personnel to attend to such victims. Finally, coordination among localities, states, public health officials, critical infrastructure entities, and the private sector is essential to enhance capabilities to detect a

potential pandemic, locate its origin, stop its spread, and mitigate the repercussions on society (Homeland Security Council, 2005).

Fusion centers. Some commonalities among the aforementioned threats include the need for situational awareness, timely and accurate intelligence, and effective communication and collaboration among numerous agencies as multiple become involved in public health related incidents. Through information gathering and sharing practices with several partners, fusion centers provide these abilities and can help to assist in better preparedness and response practices including public health incidents.

Terrorist attacks. Weapons of mass destruction and explosives are threats that terrorists tend to utilize in order to instill fear in the public, inflict massive critical infrastructure damage, impact the economy, and cause mass casualties. In order to detect such terroristic threats, it is essential to develop timely and accurate intelligence, coordinate with local, state, and federal governments, as well as the private sector, and share information. Often nontraditional collectors of intelligence, such as the private sector and public safety, contribute to fusion centers by providing important crime-related information such as risk assessments and suspicious activity. Fusion centers, in return, combine such information with law enforcement to develop actionable intelligence. The centers continue to reevaluate existing data in context with new data in order to provide updates on patterns, trends, and potential threats. This supports their abilities to better anticipate, detect, prevent, monitor, and respond to terrorist activity. Fusion centers' information collection on other criminal activities such as illegal drug operations, fraud, money laundering, or identity theft can also assist in detecting a nexus between such crimes and potential terrorist organizations. Leveraging such information and intelligence supports the rapid identification of trends and patterns that may reflect emerging terrorist threats (DOJ, 2006). Fusion centers also

support intelligence efforts to combat terrorist attacks by coordinating with joint terrorism task forces, or operational groups, led by the FBI, that leverage a variety of resources from partner agencies to investigate and disrupt terrorist threats (DOJ, 2008).

Natural incidents. While originally developed to enhance collection, analysis, and information sharing practices to detect criminal and terrorist activity, fusion centers are expanding to include all hazards approaches. In 2008, the Center for Disease Control and Prevention developed a pilot program, BioPHusion, to test the operational capacity and potential implementation of a public health fusion center. BioPHusion was developed and tested in order to develop a network that allowed for alert verification and distribution by collecting, monitoring, and integrating disparate kinds of health information into actionable intelligence. Such measures were created to support public health and take precautions to detect potential health threats such as pandemics. Similar to other fusion centers, BioPHusion maintains situational awareness. It is also a source of public health information for use by other agencies, such as the Department of Homeland Security. Enhancing early detection and rapid response of potentially catastrophic infectious disease outbreaks, as well as other public health emergencies, requires the integration of information among local, state, tribal, territorial, and federal partners. As public health concerns, such as pandemics, emerge, it is important to develop ways to aggregate data, access such information, and share patterns and trends with partners involved in preparing and responding to potential pandemics. Public health fusion centers can ensure the integration and exchange of biosurveillance information and enhance current capabilities to gather and analyze such data. With this data and knowledge, fusion centers would be able to disseminate information to decision makers involved in studying, preparing for, and responding to pandemics (Khan, Fleischauer, Casani, & Groseclose, 2010).

In order to develop national health security, it is necessary to develop intelligence and share information related to both human-caused and natural incidents. Building national health security requires building information sharing partnerships and leveraging one another's resources. Because fusion centers are focal points for information sharing, they can be extremely beneficial to the understanding, analysis, and dissemination of threat data related to public health. Several reports regarding public health preparedness such as the National Preparedness Guidelines and the Pandemic and All-Hazards Preparedness Act have continued to reinforce the importance of using developing information technology and information management to support quicker, large-scale, more effective, and higher-quality detection of, response to, and recovery from public health emergencies. Such practices can be developed and strengthened through the use of fusion centers, enhancing the quality and quantity of pertinent data from which to identify relevant threats (DOJ, 2011).

Leadership Challenges of Public Health

Because public health threats such as weapons of mass destruction, explosives, and pandemics require numerous personnel in preparation and response efforts, leadership can remain a challenge in public health scenarios. Personnel can range from law enforcement, public health officials, the private sector, and the public. Public health incidents require teamwork in order to prevent attacks, protect infrastructure and people, minimize damage, and expedite recovery (GPO, 2008). With so many different personnel involved in public health incidents with different roles and responsibilities, however, it can be difficult to manage such incidents and ensure effective response efforts.

Within the varying agencies and sectors, leadership from the healthcare industry is key to an effective response. Whether an attack includes weapons of mass destruction or explosives or

the spread of a pandemic, public health personnel play a vital role in response efforts. Doctors, nurses, EMS personnel, and critical care physicians all assist in these incidents that often lead to surge capacity within hospitals where patients require immediate assistance. Leaders within different hospitals must also be linked to assist patient transfers and provide mutual aid (Department of Health and Human Services, n.d.).

Effective preparedness and response efforts demand an established leadership structure with clear organizational responsibilities. In order to organize roles and responsibilities, including leadership, it is crucial to develop a hospital incident command system (HICS) in the event of an emergency. HICS is a widely used emergency management system for health care facilities that provides a chain of command that can quickly mobilize. Identifying the appropriate individuals to make decisions is crucial in a fast-speed disaster that can stem from incidents such as weapons of mass destruction, explosives, and pandemics. HICS allows such personnel to ensure accountability of position functions, allow for a flexible response to certain emergencies, improve documentation of facility actions throughout the emergency, provide a common language to facilitate outside personnel assisting, effectively manage an incident, and develop response checklists for senior leadership. Most importantly, those maintaining leadership roles within the incident management system must be knowledgeable of operations of other hospitals and community disaster responses as well as be trained in effectively managing incidents that require collaboration among numerous personnel in public health and public safety (Department of Health and Human Services, n.d.).

Conclusion

Impending public health threats such as weapons of mass destruction, explosives, and pandemics remain a serious concern for the United States. As these threats expand and grow, it is

crucial to develop and implement efficient preparedness and response efforts. Fusion centers, in particular, can be beneficial to preparedness and response practices for public health related incidents. Their abilities to provide situational awareness to a locality, develop sound and accurate intelligence, inform decisions based on developed information, and collaborate among numerous public safety partners makes them a valuable resource to public health officials. By collaborating and cooperating with fusion centers, public health officials can better detect, mitigate, and prevent public health related incidents.

Conclusion

After September 11th 2001, the need for better communication and information sharing practices among law enforcement partners became very evident (National Commission on Terrorist Attacks, 2004). Recognizing a communication gap among law enforcement agencies, the Department of Homeland Security (DHS) and the Department of Justice (DOJ) developed several new fusion centers to serve a critical role in identifying, analyzing, and sharing emerging threat-related information among law enforcement partners (FBI, 2009).

Today, fusion centers remain a valuable asset to local law enforcement agencies and homeland security personnel as they gather and analyze information, develop actionable intelligence, and share such intelligence with several partners (DHS, 2017c). Remaining in various urban areas, local fusion centers retain situational awareness allowing them to assist local law enforcement efforts as well as contribute to the national threat picture (DHS, 2017d). Their partnerships with numerous law enforcement agencies and homeland security personnel allow them to alleviate deconfliction problems, develop connections in investigations, and identify threats in an efficient and effective manner.

Because local fusion centers play a crucial role in supporting criminal and terrorist investigations, it is valuable to continue to enhance their information sharing practices. My two-part strategy consisting of strengthening current partnerships among fusion center analysts, local law enforcement personnel, and local FBI joint terrorism task forces, and developing and implementing a standardized training program for intelligence analysts aims to strengthen communication among law enforcement and enhance analysis and dissemination of intelligence. Through the use of efficient managers, strategic planning and budgeting, policy development and analysis, and information technology protection, the aforementioned plans can be developed and

implemented to strengthen communication and enhance uniformity of proficiencies and practices among all fusion centers.

In implementing the plans to enhance information sharing among fusion centers, procedures are needed to not only generate the seamless exchange of information among law enforcement partners, but to ensure that such practices and procedures are guided by the Constitution and abide by international human rights. Developing such procedures reassures the public that in the process of enhancing information sharing practices among fusion centers, Americans' individual liberties will remain protected. This also allows the public to provide greater support for fusion centers and recognize their value in protecting the community.

Not only have fusion centers had success in criminal and terrorist investigations (DHS, 2015e), but they continue to expand their resources and capabilities in gathering information and developing intelligence to other areas of expertise as well. They have begun to expand their capabilities to an all-hazards approach focusing on developing partnerships with various disciplines including public health and emergency management (Harris, 2008). They also collaborate with the private sector to aid in reducing risks to the community (DHS, 2014). The expansion of fusion centers' information sharing partners demonstrates their value in being able to assist the community in many ways and protect them from various threats and disasters. Not only have fusion centers continued to expand their connections with partners within the U.S., but they have also developed connections with law enforcement in other countries. As seen with one of America's allies in the Middle East, Saudi Arabia seems to be moving in the direction of developing similar information sharing centers as they have already established "fusion cells" where various partners, including Saudi Arabian intelligence officials and U.S. law enforcement

personnel, can work together to investigate and interdict terrorism plots (Saudi Arabia & Counterterrorism April, 2017).

As criminals and terrorists continue to find new ways to attack, fusion centers' ability to remain at the forefront of information gathering and disseminating among agencies can assist in various forms of crimes. Cybercrimes, for example, continue to expand as advancements in technology and both the availability and access to information grow. Such newly emerging crimes can emanate from terrorists or nation states threating local communities and the security of the United States. Fusion centers' situational awareness and contact with local law enforcement officials can greatly assist in detecting a potential threat to the community and subsequently responding to it. Furthermore, they can disseminate intelligence forewarning other centers, agencies, and law enforcement officials of the potential threats in a timely and efficient manner. It is this unique ability of recognizing various forms of threats, gathering and analyzing information, and disseminating intelligence among law enforcement partners that helps to influence rapid response efforts and prevent the threat.

As new, greater threats continue to transpire, enhancing fusion centers' information sharing capabilities becomes more and more important. Their situational awareness, partnerships with law enforcement personnel, and ability to gather, analyze, develop, and share actionable intelligence makes them invaluable in being able to protect communities. By continuing to improve information sharing among local fusion centers and leveraging their resources and capabilities to exchange information with several partners, fusion centers can better identify, mitigate, and prevent threats impacting public safety and the security of the country.

References

Al-Muharrmi, Z. (2010). Understanding the Influenza A H1N1 2009 pandemic. *Sultan Qaboos University Medical Journal, 10*(2), 187-195. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3074714/

Ambler, T. E. (2017). *Strategic issues: The pivotal process for strategic success.* Retrieved from http://www.cssp.com/CD0799/ProcessForStrategicSuccess/

American Civil Liberties Union. (2019). *What's wrong with fusion centers - Executive summary.* Retrieved from https://www.aclu.org/report/whats-wrong-fusion-centers-executive-summary

Barishansky, R. M., & Komansky, S. J. (2014). Fusion centers and the public health advantage. *Domestic Preparedness.* Retrieved from https://www.domesticpreparedness.com/healthcare/fusion-centers-the-public-health-advantage/

Bryson, J. M. (2004). *Strategic planning: For public and nonprofit organizations 3rd edition: A guide to strengthening and sustaining organizational achieving.* San Fransisco, CA: John Wiley & Sons.

Carter, D. L. (2006). *The intelligence fusion process for state, local and tribal law enforcement.* Unpublished doctoral dissertation, Michigan State University, Michigan. Retrieved from https://www.ncirc.gov/documents/public/intelligence_fusion_process.pdf

Carter, D. L., & Carter, J. G. (2009). The intelligence fusion process for state, local and tribal law enforcement. *Criminal Justice and Behavior, 36*(12), 1-39. https://scholarworks.iupui.edu/bitstream/handle/1805/3855/Carter-2009-Intelligence-Fusion.pdf?sequ

Chandra, A., Acosta, J., Stern, S., Uscher-Pines, L., Williams, M., Yeung, D., Garnett, J., & Meredith, L. (2011). Building community resilience to disasters: A way forward to enhance national health security. *RAND Health.* Retrieved from https://www.rand.org/content/dam/rand/pubs/technical_reports/2011/RAND_TR915.pdf

Chikere, C. C., & Nwoka, J. (2015). The systems theory of management in modern day organizations – A study of aldgate congress resort limited Port Harcourt. *International Journal of Scientific and Research Publications, 5*(9), 1-7. Retrieved from http://www.ijsrp.org/research-paper-0915/ijsrp-p4554.pdf

Community Literacy of Ontario. (2013). *Assessing mission, mandates and values*. Retrieved from http://literacybasics.ca/strategic-planning/strategic-planning-assesssment/assessing-mission-mandates-and-values/

Denning, D. (2017). Cyberwar: How Chinese hackers became a major threat to the U.S. *Newsweek.* Retrieved from https://www.newsweek.com/chinese-hackers-cyberwar-us-cybersecurity-threat-678378

Department of Energy Office of Energy Assurance. (2001). *Vulnerability assessment and survey lessons learned and best practices.* Retrieved from https://www.hsdl.org/?view&did=446049

Department of Health and Human Services. (n.d.). *Updated in a moment's notice: Surge capacity for terrorist bombings.* Retrieved from https://www.acep.org/globalassets/uploads/uploaded-files/acep/by-medical-focus/disaster/inamomentsnotice.pdf

Department of Homeland Security. (2008). *National response framework*. Retrieved from https://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf

Department of Homeland Security. (2014). *Facilitating private sector engagement with fusion centers*. Retrieved from https://www.dhs.gov/sites/default/files/publications/Facilitating%20Private%20Sector%0Engagement%20with%20Fusion%20Centers.pdf

Department of Homeland Security. (2015a). *2010 Fusion centers success stories.* Retrieved from https://www.dhs.gov/2010-fusion-center-success-stories

Department of Homeland Security. (2015b). *2013 Fusion centers success stories.* Retrieved from https://www.dhs.gov/2013-fusion-center-success-stories

Department of Homeland Security. (2015c). *2015 fusion center success stories.* Retrieved from https://www.dhs.gov/2015-fusion-center-success-stories

Department of Homeland Security. (2015d). *2014 fusion center success stories.* Retrieved from https://www.dhs.gov/2014-fusion-center-success-stories

Department of Homeland Security. (2015e). *2012 fusion center success stories.* Retrieved from https://www.dhs.gov/2012-fusion-center-success-stories

Department of Homeland Security. (2015f). *Fusion center success stories*. Retrieved from https://www.dhs.gov/fusion-center-success-stories

Department of Homeland Security. (2016). *Fusion centers and joint terrorism task forces.* Retrieved from https://www.dhs.gov/fusion-centers-and-joint-terrorism-task-forces

Department of Homeland Security. (2017a). *Fusion center locations and contact information.* Retrieved from https://www.dhs.gov/fusion-center-locations-and-contact-information

Department of Homeland Security. (2017b). *Information technology sector*. Retrieved from https://www.dhs.gov/information-technology-sector

Department of Homeland Security. (2017c). *National network of fusion centers fact sheet.* Retrieved from https://www.dhs.gov/national-network-fusion-centers-fact-sheet

Department of Homeland Security. (2017d). *State and major urban area fusion centers.* Retrieved from https://www.dhs.gov/state-and-major-urban-area-fusion-centers

Department of Homeland Security. (2018a). *Critical infrastructure sectors.* Retrieved from https://www.dhs.gov/critical-infrastructure-sectors

Department of Homeland Security. (2018b). *Fusion centers' support of national strategies and guidance.* Retrieved from https://www.dhs.gov/topic/fusion-centers-support-national strategies-and-guidance

Department of Homeland Security. (2018c). *Homeland security grant program (HSGP).* Retrieved from https://www.dhs.gov/homeland-security-grant-program-hsgp

Department of Homeland Security. (2018d). *Resources for fusion centers*. Retrieved from https://www.dhs.gov/resources-fusion-centers

Department of Homeland Security. (2018e). *2017 national network of fusion centers: Final report*. Retrieved from https://www.hsdl.org/?view&did=817528

Department of Homeland Security. (n.d.). *Fiscal year (fy) 2018 homeland security grant program (hsgp) notice of funding opportunity (nofo) – Key changes.* Retrieved from https://www.fema.gov/media-library-data/1526579109644 331329c9506686b5add4761aa2e37dc0/FY_2018_HSGP_Key_Changes_FINA _508.pdf

Department of Homeland Security Office of Inspector General. (2010). *Information sharing with fusion centers has improved, but information system challenges remain.* Retrieved from https://www.hsdl.org/?view&did=13906

Department of Justice. (2006). *Fusion center guidelines: Developing and sharing information and intelligence in a new era.* Retrieved from https://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf

Department of Justice. (2008). *Baseline capabilities for state and major urban area fusion centers: A supplement to the fusion center guidelines.* Retrieved from https://www.fema.gov/pdf/government/grant/2010/fy10_hsgp_fusion.pdf

Department of Justice. (2009). *Fusion center technology guide: DHS/DOJ fusion process technical assistance program and services.* Retrieved from https://www.ncirc.gov/documents/public/Fusion_Center_Technology_Guide.pdf

Department of Justice. (2010a). *Common competencies for state, local, and tribal intelligence analysts.* Retrieved from https://www.ncirc.gov/documents/public/common_competencies_state_local_and_Triba_intelligence_analysts.pdf

Department of Justice. (2010b). *Fusion center privacy policy development: Privacy, civil rights, and civil liberties policy template.* Retrieved from https://it.ojp.gov/documents/d/Fusion%20Center%20Privacy%20Policy%20Development.pdf

Department of Justice. (2011). *Health security: Public health and medical integration for fusion centers*. Retrieved from https://www.hsdl.org/?abstract&did=685166

Department of Justice. (2012). *The Privacy Act of 1974 5 U.S.C. § 552a (2012).* Retrieved from https://www.justice.gov/opcl/file/844481/download

Department of Justice (2015). *Cyber integration for fusion centers: An appendix to the baseline capabilities for state and major urban area fusion centers.* Retrieved from https://www.hsdl.org/?view&did=808477

Department of Justice. (n.d.a). *Domestic security advisory council.* Retrieved from https://www.dsac.gov

Department of Justice (n.d.b). *Office of private sector*. Retrieved from https://www.fbi.gov/about/partnerships/office-of-private-sector

Department of Justice. (n.d.c). *The USA PATRIOT act: Preserving life and liberty.* Retrieved from https://www.justice.gov/archive/ll/highlights.htm

Department of State. (2017a). *Saudi Arabia 2017 crime & safety report: Riyadh*. Retrieved from https://www.osac.gov/pages/ContentReportDetails.aspx?cid=21978

Department of State. (2017b). *Saudi Arabia 2017 human rights report.* Retrieved from http://www.humanrightsvoices.org/assets/attachments/documents/2017sdsaud.pdf

Department of State. (n.d.). *Chapter 2: Country reports: Middle East and North Africa.* Retrieved from https://www.state.gov/j/ct/rls/crt/2016/272232.htm

Devine, T. (2014). An examination of the effectiveness of state and local fusion centers toward federal counterterrorism efforts. *Intelligence and National Security Studies University of Texas at El Paso.* Retrieved from https://academics.utep.edu/Portals/4302/Student%20research/Capstone%20projects/Devine_State%20and%20Local%20Fusion%20Centers.pdf

Dhurde, S. R., & Deshpande, A. (2014). Detecting critical link and critical node vulnerability for network vulnerability assessment. *International Journal of Innovative Research in Computer and Communication Engineering, 2*(11), 6732-6737. Retrieved from

http://www.ijircce.com/upload/2014/november/37_Detecting.pdf

Director of National Intelligence. (2011). *U.S. national intelligence: An overview.* Retrieved from https://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf

Fazzini, K. (2018). Why the US government is so suspicious of Huawei. *CNBC.* Retrieved from https://www.cnbc.com/2018/12/06/huaweis-difficult-history-with-us-government.html

Federal Bureau of Investigation. (2009). *Fusion centers: Unifying intelligence to protect Americans.* Retrieved from https://archives.fbi.gov/archives/news/stories/2009/march/fusion_031209

Federal Bureau of Investigation. (2018). Chinese hackers indicted. *News*. Retrieved from https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018

Federal Bureau of Investigation (n.d.). *Cyber crime*. Retrieved from https://www.fbi.gov/investigate/cyber

FEMA. (2011). *A whole community approach to emergency management: Principles, themes, and pathways for action*. Retrieved from https://www.fema.gov/media-library data/20130726-1813-25045-0649/whole_community_dec2011__2_.pdf

FEMA. (2018). *Homeland security grant program.* Retrieved from https://www.fema.gov/homeland-security-grant-program

Fisher, E. A. (2016). Cybersecurity issues and challenges: In brief. *Congressional Research Service.* Retrieved from https://fas.org/sgp/crs/misc/R43831.pdf

Gercke, M. (2012). *Understanding cybercrime: Phenomena, challenges and legal response.* Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Gerencser, M., Van Lee, R., Napolitano, F., & Kelly, C. (2008). *Megacommunities: How*

Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together. New York: Palgrave Macmillan.

Gerras, S. J., & Clark, M. (2011). *Effective team leadership: A competitive advantage*. U.S. Army War College, Department of Command, Leadership & Management. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a595113.pdf

Gertz, B. (2019). China using OPM records for spying. *The Washington Free Beacon.* Retrieved from https://freebeacon.com/national-security/china-using-opm-records-for-spying/

Government Publishing Office. (2008). *Compilation of homeland security presidential directives (HSPD).* Retrieved from https://www.govinfo.gov/content/pkg/CPRT-110HPRT39618/pdf/CPRT-110HPRT39618.pdf

Gursky, E., Inglesby, T. V., & O'Toole, T. (2003). Anthrax 2001: Observations on the medical and public health response. *Biosecurity and bioterrorism: Biodefense strategy, practice, and science, 1*(2), 97-110. Retrieved from http://www.centerforhealthsecurity.org/our-work/pubs_archive/pubs-pdfs/2003/2003-06-15-anthrax2001observations.pdf

Harrell, P. (2018). *China's non-traditional espionage against the United States: The threat ad potential policy responses*. Retrieved from https://www.cnas.org/publications/congressional-testimony/chinas-non-traditional-espionage-against-the-united-states-the-threat-and-potential-policy-responses

Harris, B. (2008, August 19). Fusion centers may strengthen emergency management. *Government Technology*, 1-9. Retrieved from http://www.govtech.com/security/Fusion-Centers-May-Strengthen-Emergency-Management.html#

Hodai, B. (2013, May 22). The homeland security apparatus: Fusion centers, data mining and private sector partners. *The Center for Media and Democracy's PR Watch.* Retrieved

from https://www.prwatch.org/news/2013/05/12122/homeland-security-apparatus-fusion-centers-data-mining-and-private-sector-partner

Homeland Security Council. (2005). *National strategy for pandemic influenza.* Retrieved from https://www.cdc.gov/flu/pandemic-resources/pdf/pandemic-influenza-strategy-2005.pdf

Jinghua, L. (2019). *What are China's cyber capabilities and intentions?* Retrieved from https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734

Johnson, B. D. (2010, May 12). *What's the different between mission and vision?* Retrieved from https://www.youtube.com/watch?v=b2MyaR0gMo0

Jones, G. R. (1994). Chapter 2: Stakeholders, managers, and ethics, *Organization theory, design, and change* (34-67). Pearson. Retrieved from https://blackboard.pace.edu/bbcswebdav/pid-3279152-dt-content-rid-8974048_1/courses/CRJ-603-71216.201770/Organizational%20Stakeholders.pdf

Kast, F. E., & Rosenzweig, J. E. (1972). General systems theory: Applications for organization and management. *Academy of Management Journal*, 447-465. http://www.communicationcache.com/uploads/1/0/8/8/10887248/general_system_theory-_applications_for_organization_and_management.pdf

Khan, A. S., Fleischauer, A., Casani, J., & Groseclose, S. (2010). The next public health revolution: Public health information fusion and social networks. *American Public Health Association, 100*(7), 1237-1242. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2882406/

Laskai, L., & Segal, A. (2019). A new old threat. *Council on Foreign Relations.* Retrieved from https://www.cfr.org/report/threat-chinese-espionage

Lewis, T. G. (2006). Risk analysis. In T. G. Lewis (Eds.), *Critical infrastructure protection in homeland security: Defending a networked nation* (145-192). Hoboken, NJ: John Wiley & Sons, Inc. Retrieved from https://onlinelibrary.wiley.com/doi/book/10.1002/0471789542

Madhav, N., Oppenheim, B., Gallivan, M., Mulembakani, P., Rubin, E., & Wolfe, N. (2017). Chapter 17 pandemics: Risks, impacts, and mitigation. In D. T. Jamison, H. Gelband, S. Horton, P. Jha, R. Laxminarayan, C. N. Mock & R. Nugent (Eds.), *Diseases control priorities: Improving health and reducing poverty 3rd edition.* (pp. 315-346). Washington, DC: The World Bank. Retrieved from https://www.ncbi.nlm.nih.gov/books/NBK525302/

Masse, T., O'Neil, S., & Rollins, J. (2007). *Fusion centers: Issues and options for Congress.* Retrieved from https://epic.org/privacy/fusion/crs_fusionrpt.pdf

Mattis, P. (2012). The analytic challenge of understanding intelligence services. *Studies in Intelligence, 56*(3), 47-57. Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-3/pdfs/Mattis-Understanding%20Chinese%20Intel.pdf

McHugh, M. L. (2012). Interrater reliability: The kappa statistic. *Journal of Biochemia Medica, 22*(3), 276–282. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3900052/

Morgeson, F. P., DeRue, D. S., & Karam, E. P. (2010). Leadership in teams: A functional approach to understanding leadership structures and processes. *Journal of Management, 36*(1), 5-39. https://msu.edu/~morgeson/morgeson_derue_karam_2010.pdf

Muller, R. (2018). *Czech cyber watchdog calls Huawei, ZTE products a security threat.*

Retrieved from https://www.reuters.com/article/us-czech-huawei/czech-cyber-watchdog-calls-huawei-zte-products-a-security-threat-idUSKBN1OG1Z3

Multi-State Information Sharing & Analysis Center. (n.d.). *Services guide.* Retrieved from https://www.cisecurity.org/wp-content/uploads/2018/02/MS-ISAC-Services-Guide-eBook-2018-5-Jan.pdf

Nakashima, E. (2015). Chinese breach data of 4 million federal workers. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html?utm_term=.6fa2cdd67038

National Commission on Terrorist Attacks. (2004). *The 9/11 commission report: Final report on the national commission on terrorist attacks upon the United States.* New York, NY: W.W. Norton & Company, Inc.

National Security Intelligence. (2007). *National strategy for information sharing: Successes and challenges in improving terrorism-related information sharing.* Retrieved from https://fas.org/sgp/library/infoshare.pdf

Nationwide SAR Initiative. (n.d.). *A call to action: A unified message regarding the need to support suspicious activity reporting and training.* Retrieved from https://nsi.ncirc.gov/documents/a_call_to_action.pdf

Nenneman, M. W. (2008). *An examination of state and local fusion centers and data collection methods* (Master's thesis). Retrieved from Calhoun Institutional Archive of the Naval Postgraduate School Theses and Dissertations. https://calhoun.nps.edu/bitstream/handle/10945/4174/08Mar_Nenneman.pdf?sequence=1

Newcomer, K. E., Hatry, H. P., & Wholey, J. S. (2015). *Handbook of practical program*

evaluation: Fourth edition. Hoboken, NJ: John Wiley & Sons, Inc. Retrieved from https://homeland.house.gov/wp-content/uploads/2017/11/Committee-on-Homeland-Security-Fusion-Center-Report.pdf

Northouse, P. G. (2012). Team leadership. In S. K. Hill (Ed.), *Leadership: Theory and practice* (pp. 287-318). SAGE Publications. Retrieved from http://www.academia.edu/22270113/Leadership_Theory_and_Practice_6th_editi..

Northouse, P. G. (2013). Team leadership. In L. Cuevas Shaw, P. Quinlin, M. Stanley, M.N. White, M. Vail, E. Garner, M. Masson & K. Ehrmann (Eds.), *Leadership: Theory and practice* (pp. 287-315). SAGE Publications. Retrieved from https://in.sagepub.com/sites/default/files/upm-binaries/47444_chp_12.pdf

Olsen, E. (2008, July 9). *How to write a vision statement that inspires.* Retrieved from https://www.youtube.com/watch?v=ioY-YSOKBtY

Olsen, E. (2016, October 19). *How to perform a SWOT analysis.* Retrieved from https://www.youtube.com/watch?v=I_6AVRGLXGA

Police Executive Research Forum. (2018). *New national commitment required: The changing nature of crime and criminal investigations*. Retrieved from https://www.policeforum.org/assets/ChangingNatureofCrime.pdf

Sanger, D.E., Perlroth, N., Thursh, G., & Rappeport, A. (2018). Marriott data breach is traced to Chinese hackers as U.S. readies crackdown on Beijing. *The New York Times*. Retrieved from https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html

Segal, A. (2018). When China rules the web. *Foreign Affairs.* Retrieved from https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web

The Constitution Project. (2012). *Recommendations for fusion centers: Preserving privacy and*

civil liberties while protecting against crime and terrorism. Retrieved from https://constitutionproject.org/pdf/fusioncenterreport.pdf

Torres, J. (2014, May 24). *SMART Goals.* Retrieved from https://www.youtube.com/watch?v=q1tOQgYJEf8

United Nations. (1996-2019). *International Covenant on Civil and Political Rights.* Retrieved from https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

United Nations. (n.d.). *Universal Declaration of Human Rights.* Retrieved from http://www.un.org/en/universal-declaration-human-rights/

U.S. Const. amend. I-X, XIV.

Von Bertalanffy, L. (1972). The history and status of general systems theory. *The Academy of Management Journal, 15*(4), 407-426. http://perflensburg.se/Bertalanffy.pdf

Weimann, G. (2004). Cyberterrorism how real is the threat? *United States Institute of Peace*. Retrieved from https://www.usip.org/sites/default/files/sr119.pdf

Wyckoff, K. (2015). Solving homeland security's wicked problems: A design thinking approach. *Homeland Security Affairs, 14.* Retrieved from https://www.hsaj.org/articles/8101

Xie, K. (2018). The value of collaborative threat intelligence sharing. *Cyber Threat Alliance.* Retrieved from https://www.cyberthreatalliance.org/value-collaborative-threat-intelligence-sharing/

Yang, Z. (2017). China is massively expanding its cyber capabilities. *Center for National Interest.* Retrieved from https://nationalinterest.org/blog/the-buzz/china-massively-expanding-its-cyber-capabilities-22577

A brief orientation to dialogue. (2006). Retrieved from http://measuresofhealth.net/pdf/brief_orientation_dialogue.pdf

Beggars 'part of organized crime groups.' (2015, July 10). *Arab News.* Retrieved from http://www.arabnews.com/saudi-arabia/news/774356

Course overview. (n.d.). Retrieved from https://emilms.fema.gov/IS800c/groups/249.html

DHS addresses fusion center concerns. (2008). *Government Technology and Services Coalition's Homeland Security Today*. Retrieved from https://www.hstoday.us/industry/daily-news-analysis/dhs-addresses-fusion-center-concerns/

IT infrastructure: Hardware and software. (2013). Retrieved from http://cs.furman.edu/~pbatchelor/mis/Slides/Infrastructure%20Hardware%20and%20Software%20Week%202.pdf

Privacy and human rights: An International Survey of Privacy Laws and Practice. (n.d.). Retrieved from http://gilc.org/privacy/survey/intro.html

Right to privacy in the United States. (2017). *Laws.* Retrieved from https://constitution.laws.com/right-to-privacy

Saudi Arabia & counterterrorism April 2017 report. (2017). Retrieved from https://saudiembassyuk.co.uk/wp-content/uploads/2017/09/Counterterrorism-White-Paper-Final_UK_Single.pdf

Saudi Arabia & counterterrorism fact sheet: Fighting and defeating Daesh. (2017). Retrieved from https://www.saudiembassy.net/sites/default/files/Fact%20sheet%20-%20Fighting%20and%20Defeating%20Daesh.pdf

Saudi intelligence agencies. (2017). *Invisible Dog Investigative Journalism*,(71), 1-3. Retrieved from http://www.invisible-dog.com/saudi_intelligence_eng.html

Saudi Secret Service (Istakhbarat) Maslahat Al-Istikhbarat Al-Aammah (Global Intelligence

Department. (2000-2019). Retrieved from https://www.globalsecurity.org/intell/world/saudi/istakhbarat.htm

Summary of final report. (2014). *The New York Times.* Retrieved from https://www.nytimes.com/2004/07/22/politics/summary-of-final-report.html