CYBER SECURITY AND GOVERNMENT FUSION CENTERS

Natalie Granado, Gregory White
Center for Infrastructure Assurance and Security
The University of Texas at San Antonio
Natalie.granado@utsa.edu, Greg.White@utsa.edu

Abstract

The Department of Homeland Security has recommended the creation of State, Regional, and Community Fusion Centers. These centers, run by state and local governments, are designed to take what may seem to be disparate pieces of information on a variety of subjects and "fuse" them together to be able to recognize indicators of potential terrorist attacks. These centers are generally staffed with personnel who have intelligence and law enforcement backgrounds. Unfortunately, very few have any concept of the cyber environment and do not know what constitutes indicators of potential cyber attacks. This paper discusses the need to develop a cyber capability in fusion centers and the importance of government involvement in coordinating a state's, community's, or region's cyber defense efforts.

1. Introduction

The Department of Homeland Security (DHS) has provided $380 million to support state and local Fusion Centers. These centers, which blend law enforcement and intelligence information analysis, are designed to reduce threats in local communities by providing leaders with advance warning of pending attacks. Fusion Centers are designed to

- provide critical sources of unique law enforcement and threat information
- facilitate sharing information across jurisdictions and function
- provide a conduit between men and women on the ground protecting their local communities and state and federal agencies. [1]

Fusion Centers are intended to facilitate the two-way flow (from state and federal levels to local levels, and back) of timely, accurate, actionable information for all hazards. According to the guidelines for fusion centers jointly prepared by the Department of Justice (DOJ) and the Department of Homeland Security (DHS), a fusion center "is an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by analyzing data from a variety of sources." [2] If the fusion centers are successful, attacks will be prevented as analysts combine what may seem to be disparate pieces of information into a coherent picture pointing to threats to communities, states, and the nation.

There is little doubt that fusion centers are needed to counter threats to the nation from organizations other than the military forces from other nations. States and communities have stepped up their efforts to prepare for possible attacks using any of a number of weapons including conventional explosives as well as chemical or biological weapons. What is less understood is the potential threat that can originate from cyberspace and that target the various critical infrastructures of the nation. Without an understanding of these threats fusion centers have thus far not prepared to address these issues. The first step in preparing for them is thus to understand what can be accomplished and who the nation's potential adversaries might be in the cyber realm.

2. The Cyber Threat

Recently, tens of thousands of computers were attacked in the nation of Estonia. These systems were bombarded with tremendous amounts of network traffic in a large-scale denial of service attack. [3] Web sites were crippled across the nation and included sites run by schools, banks, and government organizations. The attacks came from systems around the world but were believe to have originated from Russia. There are a number of significant aspects to this attack. First, the attacks were launched against not just government sites but commercial entities as well.

1530-1605/08 $25.00 © 2008 IEEE

A nation engaging in a cyber conflict with another nation may target computer systems and networks for entities not normally considered targets in a conflict. Industry, critical infrastructures (such as power, water, and oil & gas) and schools may be targeted in order to cause chaos and confusion and to disrupt life for the citizens of the targeted nation. These targets exist within every community and state and are essential for normal daily activities.

The second significant aspect of the attacks in Estonia was the apparent reason for the attack. A Russian World War II memorial was moved from its location to a less prominent one. Russians living in Estonia were upset with this move as were others outside of Estonia. Shortly after the move was made the attacks, reportedly originating from Russia began. This demonstrates how seemingly insignificant events can lead what could be a very small minority of individuals to launch a cyber attack that could cripple communities, states, and even a nation. Potential attackers, capable of affecting large numbers of individuals, include not just nation-states but terrorist groups or even "hacktivists" (activists who use the Internet to broadcast their agenda).

An important issue is the extent to which the nation (or its states and communities) is susceptible to attacks from cyberspace. According to John Rollins and Clay Wilson in a 2005 Congressional report, "extensive coverage has been given to the vulnerability of the U.S. information infrastructure and to the potential harm that could be caused by a cyberattack. This might lead terrorists to feel that even a marginally successful cyberattack directed at the United States may garner considerable publicity." [5] Reports on the level of cyber preparedness by various government agencies have been produced annually. For the last two years, the average score of the agencies evaluated has been a D+. [6]

A question to ask is how likely is an attack from cyberspace by entities such as terrorist organizations? This question is hard to answer but what can be answered is whether they are aware of the possibilities that cyberspace presents. Terrorists are undoubtedly familiar with the Internet and electronic technology. Reports indicate that Al Qaeda used the Internet extensively to plan operations for the attacks of September 11, 2001. Al Qaeda is also known to have improved methods to maintain its own electronic secrecy. Internet chat software was reportedly used to communicate with at least two airline hijackers. [4] Recent natural disasters as well as the effect other terrorist attacks have had on various critical infrastructures have reinforced the potential benefits of targeting them. The attacks on the World Trade Center, for example, closed financial markets for up to a week as a result of the loss of communications links and data.

Not only do we know that Al Qaeda and other terrorist organizations understand how to use the Internet to help advance their agenda, we also know that they understand the Internet's potential as a target of attack. A 2007 article in the Sunday Times stated that "Scotland Yard has uncovered evidence that Al-Qaeda has been plotting to bring down the internet in Britain, causing chaos to business and the London Stock Exchange." [7] In addition, the Washington Times reported that "a web forum for Muslim extremists is calling on its members to organize an Islamist hackers' army to carry out Internet attacks against the U.S. government. The site has posted tips, software and links to other resources to help would-be cyber-warriors." [8] These terrorist organizations understand the potential damage that attacks on cyber infrastructures can cause. They understand the vulnerabilities that exist and our dependence on our computer systems and networks. Interestingly enough, though some might not consider an attack on the Internet such as was planned for Britain spectacular enough to be of interest to terrorist organizations, the probability of an actual cyber attack may well be on the increase. The reason for this is the success the nation has had in other areas of terrorism. As we improve our ability to prevent conventional attacks or attacks using weapons of mass destruction (WMD), terrorists will need to find other means to attack the nation. A form of attack that can be carried out far from the site of the target has a certain appeal. Cyber attacks provide this possibility.

3. Fusion Centers

As was mentioned, fusion centers were created in order to provide the capability to examine seemingly disparate pieces of information and to draw from them a picture of a pending or future attack. Fusion is the key term and, according to the DHS/DOJ Guidelines, means "turning information and intelligence into actionable knowledge." "Actionable" is the key term in this description. For fusion centers to be successful they need to not just produce vast quantities of information and reports but should instead produce knowledge that is actionable – knowledge and information that leaders can use to take actions that could prevent an attack from occurring. Again from the DHS/DOJ guidelines we read that "For purposes of this initiative, fusion refers to the overarching process of managing the flow of information and intelligence across all levels and sectors of government and private industry. It goes beyond establishing an information/intelligence center or creating a computer network. The fusion process supports the implementation of risk-based, information-driven prevention, response, and consequence management programs." [2] This passage introduces the idea that fusion centers do not just rely on government organizations but have a private industry component as well. Building upon this idea the guidelines continue and state "data fusion involves the exchange of information from different sources—including law enforcement, public safety, and the private sector—and, with analysis, can result in meaningful and actionable intelligence and information. The fusion process turns this information and intelligence into actionable knowledge." What this fundamentally means is that for fusion centers to function, they need to be gathering information not just from law enforcement and intelligence agencies but from industry and the private sector as well. To this effect, the guidelines later state "ideally, the fusion center involves every level and discipline of government, private sector entities, and the public—though the level of involvement of some of these participants will vary based on specific circumstances." This is an important concept that becomes even more critical when considering cyber issues later.

The guidelines refer to the "fusion process" several times. This process is, quite simply, the steps necessary to turn information into actionable knowledge. The fusion process will:

- Allow local and state entities to better forecast and identify emerging crime and public health trends.
- Support multidisciplinary, proactive, risk-based, and community-focused problem solving.
- Provide a continuous flow of intelligence to officials to assist in developing a depiction of evolving threats.
- Improve the delivery of emergency and nonemergency services. [1]

Building a fusion center capability is a phased process. This was true for the development of the initial creation of the fusion center concept and is equally true as entities develop their own fusion capability. The first phase is the introduction of the law enforcement and intelligence component. This is the backbone of every fusion center. The center will rely on individuals who have the training to perform an analysis of disparate data in order to form clear pictures of what might be indicated. The second phase of building a fusion capability is the incorporation of public safety elements. This primarily means incorporating inputs from traditional first responders within communities. It also includes individuals from the transportation, agriculture, and environmental protection sectors as well. The third phase in constructing a fusion center capability is the inclusion of the private sector component. This last phase is critical to the success of fusion centers. Nearly 85 percent of the critical infrastructures needed by the nation on a daily basis are found in the private sector. But it is not just the critical infrastructures found in the private sector that are included in the final phase of building a fusion capability, it also includes private citizens and their inputs. Similar to the concept of the neighborhood watch program found in communities around the nation, private citizens can aid fusion centers by maintaining a certain level of vigilance in observing when abnormal activities occur within their communities. Law enforcement personnel and first responders can't be everywhere; citizens need to shoulder some responsibility for maintaining the security of the communities in which they live.

What citizens, the private sector, and the first responder community bring to the fusion center process is the gathering of data that will be examined by the intelligence analysts who will transform the various pieces of information into the actionable knowledge that we keep referring to. For conventional attacks and weapons of mass destruction, what information is needed is a fairly well understood process. (That is not to say that it is an easy process, just that we can describe what needs to occur for the process to be successful.) In intelligence terminology, what is being searched for are the various "indicators" of a pending attack. In the cyber realm this is a different matter. Very little has been done in terms of incorporating cyber into fusion centers and little is understood about what constitutes an indication of a potential cyber attack. Put simply, what is needed is a list of the things that people should be looking for and reporting on that would serve to indicate an attack may be in the planning or early stages of the execution process.

4. Indicators of Cyber Attacks

At first glance, it may seem that we should be able to turn to the intrusion detection/prevention community in order to obtain a list of the indicators needed by fusion centers to identify pending attacks. This is partially true. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are used to identify attacks focused on a single network or organization. This is certainly useful information and would potentially be useful for a fusion center. The problem lies in the goal of the IDS/IPS versus the goal of the fusion center.

From a cyber standpoint, the fusion center is not designed to replace the use of IDS/IPS by government organizations or the private sector. Individual entities should still be conducting their own activities to protect their own computer systems and networks. In addition, fundamentally the IDS/IPS potentially detects activities too late in the attack process. What a fusion center should do in the cyber realm is to identify larger attacks that may be focused on a community in general and can also assist in the process of identifying attacks that may occur against a single sector over a longer period of time.

To accomplish detection of indicators of a pending community cyber attack will necessitate a different set of data that will need to be gathered in order to assist the fusion center in conducting its activities. An IDS/IPS is often designed to detect specific attack signatures – patterns of specific behavior that are known to be hostile in nature. In other words, certain specific vulnerabilities are known that take advantage of certain types of commands or command sequences. If one of these known patterns is observed, there is a high probability that the activity is that of an individual attempting to exploit the vulnerability. Other IDS/IPS utilize methods to identify what might be considered normal activity on a computer system or network and will look for patterns of activity that fall outside of the established norm. The first of these methods is an attempt to identify anomalous behavior and the second is an attempt to identify abnormal behavior. Both are valid IDS/IPS methods.

From a fusion center standpoint, both of these methods are still valid. The problem is now being able to identify what is considered anomalous behavior in a community as well as identifying what might be considered abnormal behavior for a given community. For the first, we would need to be able to identify specific activities that are considered "bad" and which would be indicative of somebody attempting to attack a community. We are able to accomplish this to a certain extent. We know, for example, that there are certain activities that are accomplished before an attack occurs. A certain amount of reconnaissance activity must be conducted in order for a cyber attacker to obtain the knowledge necessary to successfully conduct a cyber attack. Activities that might fall into this category, and that can be reported, include "war driving" (traveling through an area with a computer containing a wireless card searching for open wireless networks), "war dialing" (dialing phone numbers in sequence or randomly attempting to find numbers that are answered by a computer modem), ping sweeps (sending special packets to a list of potential IP addresses in order to find which addresses are actually being used by an active computer), and port scanning (sending packets across a network to identify what services are available on a specific computer). All of these activities are important from an individual organization's perspective – a company would like to know if somebody is conducting these activities because it would indicate that somebody might be interested in penetrating their computer systems or networks. From a fusion center perspective, however, it is important to know this information for a different reason. If somebody is attacking one organization, there is a chance that they might also attack another. If a broad pattern of reconnaissance activities is seen across a sector or throughout a community, it could very well indicate plans for conducting a larger scale attack are in progress. This is the sort of analysis that a fusion center would be useful for.

For the fusion process to be effective in detecting pending cyber attacks, it is necessary for security relevant information to be reported as it is for pending attacks for any other threat type. The problem in this case is that individuals and organizations are not currently accustomed to providing this sort of information to anybody outside of their organization or the sector that they are in. Part of the reason for this is a reluctance on the part of individuals to mention when they have actually had a penetration or security incident occur. There is a fear in industry that reporting incidents could have an adverse impact on a company (and, in fact, this has been the case). As a result, few companies share information freely about attacks and are just as reluctant to share information concerning the type of activities that they may be observing. Another reason for this reluctance is the feeling that by sharing this type of information, knowledge about the organization's security posture might be obtained. The fear is that this, by itself, could lead to potentially successful attacks. This general reluctance is a reality and it is going to be a major obstacle that must be dealt with. It is imperative for the successful implementation of a cyber capability in fusion centers that this problem be overcome.

5. An Example

To illustrate the type of information that needs to be shared and how this can be used in the fusion process, it is useful to look at an example. As was mentioned, war driving is an activity that is performed by individuals attempting to locate open wireless networks that can be potentially exploited. The tools needed to accomplish this activity can be readily obtained from off of the Internet. Because of the tools can be easily obtained, this sort of activity is constantly occurring and is considered by many to not be of much interest. It is certainly currently not the type of activity that most law enforcement agencies instruct their officers to report on if seen and it is certainly not currently considered by most states to be important enough to transmit warnings throughout the state if this type of activity is occurring.

For our example, however, suppose that this type of activity is seen occurring in one community outside of a specific type of facility, say a power or water utility facility. Again, people are not trained to report war this type of activity to anybody at the state level. If, however, this activity was seen in one community on one day, then two other communities the next, and several more on a third day, it might very well point to a pattern of activity that might indicate an inordinate amount of interest in the facilities and might in fact indicate that there is a possible pending cyber attack on these critical infrastructures. It will not be possible to identify this activity, however, if nobody reports it and fusion centers are not trained in what to do with cyber indicators. Knowing what to report is the first step. Knowing who to report this information to is the next critical step.

6. State and Community Information Sharing

In order to envision how sharing of information regarding a potential cyber attack might take place, it is useful to examine information sharing efforts within states and communities for other areas of security. Since the attacks of September 11, 2001, there has been a concerted effort to establish better sharing mechanisms between local, state, and federal entities so that the mistakes (or missed opportunities) that occurred before the attack do not happen again. Effective prevention requires information and intelligence fusion as a cooperative process at all levels of government to ensure the flow of intelligence can be managed to support the identification of emerging threats.

In a 2004 research study at the Naval Postgraduate School, Robert Flowers examined the information sharing efforts of one state, Utah. Examination of information sharing issues within Utah is important because of the lessons that were learned during the development and execution of the 2002 Olympics in and around Salt Lake City. In his report, Flowers stated that “three cultural characteristics of the public safety community pose significant problems for efforts to improve the gathering and flow of homeland security-related information challenges for information initiatives”. [9] He went on to describe these three problems which are as applicable to a cyber information sharing initiative as they are to more conventional security disciplines. The three problems were:

> 1. Even when seemingly reasonable changes are made in the way that information is supposed to be gathered and distributed, the lack of trust between the people in that redesigned system will sabotage its actual effectiveness.
> 2. People in the information system are often subject to “groupthink;” that is, they lose their ability for independent thought and judgment, and instead follow the herd in resisting efforts for change.
> 3. Officials are prone to parochialism. They view problems from a narrow, local perspective, rather from the bigger picture of State and national requirements for homeland security. [9]

A significant finding in Flower’s study was a general lack of trust in the federal, and even state, government by local officials. This has tremendous implications for any program hoping to establish channels of effective information sharing. This lack of trust in government is also certainly found in both citizens and the cyber community as well – both of whom will be important to a cyber information sharing initiative. Flowers noted that significant efforts had been made in the infrastructure needed for sharing information at the state and federal levels. The weak link in the infrastructure was at the county and local levels where the distrust was also greatest.

Interestingly enough, the other major factor affecting the adoption of an effective information sharing mechanism in Utah outlined by Flowers in the report was trust. Flowers mentioned that trust was mentioned more often by officials in Utah as being an important factor and that trust directly affected the willingness of officials to commit to or participate in state initiatives. A major factor affecting trust was communication – a problem routinely reported by everyone. Local and county leaders repeatedly complained about not being included in early information sharing initiatives in Utah which left them with the feeling that they were not important and not valued as part of the initiative. This in turn caused them to be reluctant to adopt and participate in these earlier programs. Flowers pointed out that it is in these "human" elements of trust and communication that leaders need to focus when developing an information sharing program. In developing an effective cyber information sharing and fusion process these same factors will be present. Individuals at all levels from which information will be gathered need to be involved in the development process in order to foster a feeling of trust in the government entities that will be asking for participation in the program. To not include all levels up front and to then later attempt to dictate or mandate specific information sharing mechanisms will lead to the same distrust and lack of support that was seen in Utah. Government leaders should learn from their experience.

In another report, also out of the Naval Postgraduate School, William Forsyth emphasized the need for a cooperative process at all levels of government for effective information sharing. [10] In his study, Forsyth examined information sharing initiatives in three areas: Arizona, Georgia, and Los Angles. Forsyth points out that

> "after September 11, 2001, most state and local agencies looked to the federal government for support, leadership, and intelligence information that would be useful in defending ourselves against another terrorist attack. While the federal government has made efforts to improve the broader dissemination of information to state and local agencies, many still feel that the information provided by the federal government is dated, irrelevant to local issues, and generally not useful for local communities." [10]

This feeling of irrelevance affects the willingness of individuals at the local level to participate in information sharing initiatives. A common statement heard by the authors of this paper in their work with communities around the nation is that information sharing is one-way communication – that they are expected to provide information to federal agencies (such as the Federal Bureau of Investigation) but that they never get any useful information from them – the same problem outlined by Forsyth.

In his study, Forsyth examined the information sharing initiatives of Arizona focused in the Arizona Counter-Terrorism Information Center (ACTIC), a 24-hour entity tasked with among other things:

- Providing tactical and strategic intelligence collection, analysis, and dissemination support to local, state, and federal law enforcement agencies;
- Maintaining and disseminating an on-going threat analysis for the State of Arizona and its critical infrastructure;
- Providing informational support to the Governor and other critical governmental leaders;
- Maintaining a secure web site to disseminate intelligence and critical information accessible to all law enforcement and first responder agencies;
- Maintaining the Anti-Terrorism Information Exchange (ATIX) secure web site portal for the dissemination and exchange of information to law enforcement and public and private stakeholder agencies that support homeland security efforts;
- Functioning as the state's central point of dissemination for homeland security threat level conditions and other information generated by the FBI, U.S. Attorney's Office and other state, local, tribal, and federal agencies;
- Maintaining contact with the FBI Joint Terrorism Task Force, the U. S. Attorney's Office of Anti-Terrorism Task Force, and other state, local, and federal law enforcement agencies in on-going investigations;
- Providing necessary training on intelligence function and the role of law enforcement and private citizenry in guarding against terrorist attacks. [10]

Forsyth also reported on the efforts in Georgia to establish the Georgia Information Sharing and Analysis Center (GISAC). Forsyth reported the mission of the GISAC is

> "…to serve as the focal point for the collection, assessment, analysis, and dissemination of terrorism intelligence

> information relating to Georgia. GISAC was not intended to replace or duplicate the counter-terrorism duties of the Federal Bureau of Investigation, but rather to enhance and facilitate the collection of intelligence information from local and state sources, and to integrate that intelligence information into a system that will benefit homeland security and counter-terrorism programs at all levels." [10]

Finally, Forsyth also reported on the efforts in Los Angeles to create the Los Angeles County Terrorism Early Warning (TEW) Center. This center is important because it was the first operational fusion center in the country and "was created to form a countywide group that was capable of a highly coordinated response to acts of terrorism, based on careful assessments of information, intelligence and detailed planning." [10] Unlike the other two efforts, the TEW was actually established prior to the events of September 11, 2001 instead meeting for the first time in October 1996. This meant that they were operational during the first anthrax attack alerts in 1998 and the events surrounding the Y2K cyber problems. Possibly as a result of its longer existence, the TEW is recognized in the Los Angeles area as being highly effective in fostering cooperation, teamwork, and information sharing between agencies in Los Angeles County and the State of California.

Interestingly, while Forsythe discusses the role of information technology (IT) at several points in the paper, handling cyber incidents is not discussed. All entities discussed in the study emphasize the importance of IT in the collection and sharing of information. The use of common IT tools such as databases for storing and retrieving information used in the analysis of events is frequently mentioned. The organizations analyzed in the study all focused primarily on the analysis of information by government entities such as law enforcement. The methods used to obtain the information utilized by fusion centers was not discussed beyond explaining the need to work closely with organizations and citizens in order to establish the trust needed to foster communication. In the cyber arena there exist several entities that are not normally considered part of the first responder community but which are important as targets from which attacks can be launched. Examples include academia and industry. In current information sharing initiatives, these sectors are not normally considered an important element and the necessary communication channels mentioned do not exist.

While individuals in the cyber community may not be familiar with the concept and importance of fusion centers, most are aware of the various Information Sharing and Analysis Centers (ISACs) that exist for the critical infrastructures. While not performing the exact same function as a fusion center, ISACs and fusion centers do share the goal of fostering information sharing between entities. In the case of the ISACs, this sharing is accomplished within the sector that the ISAC oversees. Cross-sector information sharing has not been as robust.

Unlike most fusion centers, a major thrust of the sector-based ISACs is cyber security. There are ISACs created for most of the critical infrastructures with an ISAC Council that brings them together to discuss issues important to all sectors. While the original concept of an ISAC was to create them for the various sectors represented by the critical infrastructures, other entities can implement them as well. As was previously mentioned, the State of Georgia created its own ISAC (the GISAC) which was designed to perform the functions of a fusion center for the state. A more conventional ISAC, the Multi-state ISAC (MS-ISAC), has been created with representation from all 50 states as well as the District of Columbia. The goal of the MS-ISAC is to

> "…provide a common mechanism for raising the level of cyber security readiness and response in each state and with local governments. The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure from the states and providing two-way sharing of information between and among the states and with local government." [11]

As can be seen, while the function of the ISACs and fusion centers overlaps in many ways, the level of understanding of cyber as a threat varies dramatically. Fusion centers tend to be focused more on the law enforcement (and government) communities and concentrate on areas considered more "traditional" for terrorist attacks (e.g. conventional explosives, chemical or biological weapons) while ISACs recognize cyber as a major focus. At the same time, most ISACs do not have the intelligence analysis capability that is found within the fusion centers. What is needed is a combination of these two entities.

7. Fusion Centers, Security, and eGov

The amount of overlap between fusion centers and ISACs would indicate the need for one or the other but not both. With the emphasis in fusion centers on all-source intelligence (i.e. information from any source no matter what the type) it would seem that they are the natural entity to focus information sharing initiatives on. This does not mean that there is no place for the sector-based ISACs, but that there is no need for community or state ISACs. There may still be offices within states that deal directly with the MS-ISAC, state departments handling information technology for example, but a state ISAC that would handle cyber incidents is probably not required. Instead, the fusion centers with their all-source focus should be trained to collect information on cyber security relevant events so that they can perform intelligence analysis on this information to detect possible pending cyber attacks. The importance of this increases as more government functions are moved to an eGovernment environment.

Implementation of eGovernment functions necessitates a certain level of computer security be implemented. Security in this case takes two forms. The security of eGovernment (and other state IT functions) itself needs to be ensured. At the same time, a fusion center, as a government entity, which includes a cyber security mission is taking on the mission of protecting the state/community from cyber-based attacks. Since attacks on a state/community can focus on any of the critical infrastructures (private or public), this means the sharing of information across all levels of government as well as industry and the citizens is necessary.

A prime concern of any entity conducting information sharing on cyber-based attacks is the potential amount of information that could be generated. Probes are conducted on a daily basis of Internet connected systems on a daily basis. Being able to discern which probe is coming from a possible terrorist as opposed to a curious high school student or a disgruntled government employee is impossible without correlation of additional information. Determination of the metrics that fusion centers can use to be able to spot pending cyber attacks is a critical research area. Is the mere fact that a certain system is being probed a critical indicator? Probably not, since any system connected to the Internet is going to be subjected to numerous probes. Is it then the source of the probe that might indicate a possible pending attack? This could be the case, but only if the potential attacker has not attempted to hide their tracks which, for intelligent adversaries, is not likely the case. Is it the amount of probes or probes of specific services? Again, this could be an indicator of an attack but only if we knew what to look for and if the probe was not "lost" in the number of other probes that are likely occurring. Is it then a combination of these factors along with possible other indicators within the state/community or within the IT/security industry? This is likely the case and just scratches the surface of the challenge posed in attempting to spot the indicators of a pending cyber attack.

As can be imagined, the amount of information that could potentially be sent to a fusion center to address the cyber mission is staggering. In fact, it is most likely unmanageable with the resources that fusion centers have available. For a fusion center to take on this mission requires three things: 1) An understanding of the cyber threat and environment by fusion center personnel; 2) A determination of what information (or subset of information) needs to be gathered at the fusion center in order to detect patterns of activity that indicate a pending or current attack; and 3) Automated systems which can take on the information gathering and first level of analysis role. The first of these three items is the easiest to address. Training on the cyber security threat to communities, states, and the nation exist already. Some work would need to be done to tailor this to the needs of fusion centers but the basic information already exists. The other two items, however, are potential areas for research.

Many of the issues that face more traditional eGovernment systems will be faced by researchers creating systems to help with this problem. One of the most significant is citizen trust in government systems. Citizen trust in the privacy and reliability of information is always a concern with eGovernment and will be a major factor in the acceptance of a system that will monitor community assets for information on pending cyber attacks. How reliable will the system be? How do private citizens know that the government isn't gathering information on them to be used in ways not originally intended? How do private companies know that the privacy of information relating to possible security vulnerabilities in their systems will not be released or made available to competitors who could use this information for a financial advantage? In addition, issues relating to the storing and retrieval of a vast amount of data needs to be addressed. Establishing cyber security-capable fusion centers is not an easy problem but it is one that needs to be addressed and it is one that provides a number of research possibilities.

8. Conclusion

Fusion centers are being established in communities, states, and regions throughout the country. These are important tools in the ongoing fight against terrorism as they provide the capability to analyze pieces of information to obtain patterns of activity that indicate possible attacks on various entities. Currently, cyber issues are not a concern of fusion centers as the cyber threat is a growing and currently not well understood threat. This needs to change, however, as there is ample evidence that various terrorist organizations are well aware of the potential that cyber attacks bring to the equation.

For cyber issues to be included in fusion centers, center personnel will need to be trained on what they should be looking for. Before this can occur, however, a list of potential indicators of possible cyber attacks needs to be established. These indicators may include the type of indicators currently used by individual intrusion detection and prevention systems but will also need to include higher-level indicators that would show when an attack on a community or state might be pending.

Fusion requires information, thus an effective information sharing program is an essential prerequisite for a fusion capability. Along with an information sharing program there is a need for automated means to collect and analyze the information gathered. Introduction of such an automated mechanism will meet with some of the same issues that face the introduction of many eGovernment systems.

Finally, for these efforts to succeed, individual organizations, and even individual citizens within a community, need to be trained on what their roles are in terms of reporting cyber incidents and events. This is a tricky issue as too much information flooding into a fusion center will only serve to potentially hide more important indicators which can complicate the issue for the intelligence analysts. Without the information, however, it will not be possible for the analysts to produce the "actionable knowledge" that is the goal of fusion centers and to prevent attacks from occurring. The challenge will be to be able to identify the possible indicators that are important in spotting cyber attacks but creating a way to limit them or to make them accessible only when needed.

It was not mentioned in this paper, but another area of possible fertile research, is the identification of cyber indicators that could be combined with non-cyber indicators to identify pending cyber or other attacks. This paper has dealt only with cyber attacks but it is very likely that future attacks may incorporate multiple avenues of attack. Cyber needs to not only be considered but considered in conjunction with other threats.

9. References

[1] Department of Homeland Security, "State and Local Fusion Centers", available at http://www.dhs.gov/xinfoshare/programs/gc_1156877184684.shtm, September 14, 2006
[2] Department of Justice and the Department of Homeland Security, Fusion Center Guidelines Developing and Sharing Information and Intelligence in a New Era, p. 2.
[3] Jeremy Kirk, "Estonia recovers from massive denial of service attack", IDG News Service, Inforworld, available at http://www.infoworld.com/article/07/05/17 /estonia-denial-of-service-attack_1.html, May 17, 2007
[4] Clay Wilson, "Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress", CRS Report RL32114, Updated April 1, 2005, p. 18
[5] John Rollins and Clay Wilson, "Terrorist Capabilities for Cyber Attack: Overview and Policy Issues", CRS Report RL33123, October 20, 2005, p. 4.
[6] Anne Broache, "DHS scores F on cybersecurity report card.", C/net, news.com, March 16, 2006
[7] David Leppard, "Al-Qaeda plot to bring down UK Internet", Sunday Times, March 11, 2007
[8] Shaun Waterman, "Islamists seek to organize hacker's jihad in cyberspace", The Washington Times, August 26, 2005
[9] Robert Flowers, "Strategies to Build a Trusted and Collaborative Information Sharing and Homeland Security Environment in Utah", Masters Thesis, Master of Arts and Security Studies, Naval Postgraduate School, June 2004.
[10] William Forsythe, "State And Local Intelligence Fusion Centers: An Evaluative Approach In Modeling A State Fusion Center", Masters Thesis, Master of Arts and Security Studies, Naval Postgraduate School, September 2005.
[11] The Multi-State Information Sharing and Analysis Center (MS-ISAC), http://www.msisac.org/