Intelligence Support to Critical Infrastructure Protection

A White Paper prepared by the AFCEA Intelligence Committee

October 2008

AFCEA

Serving Intelligence Professionals and their Community

Intelligence Support to Critical Infrastructure Protection

Table of Contents

Purpose and Overview

The Intelligence Committee of the Armed Forces Communications and Electronics Association (AFCEA) is pleased to present this white paper, part of a series[1] focused on the future of the Intelligence Community. These white papers, and the AFCEA intelligence symposia they accompany, are intended to contribute substantively to the ongoing national discussion on strengthening our nation's intelligence capabilities. Normally the Committee's papers are released in advance of the AFCEA Spring and Fall Intelligence Symposia to support and enrich the discussion that takes place during those events. In recognition of the fact that the Critical Infrastructure Protection Community, particularly the private sector, is a new customer for the Intelligence Community, this paper was released after the 2008 Fall Intelligence Symposium to benefit from the symposium discussion and to check the paper's assumptions against the reality in which the Critical Infrastructure Protection Community operates.[2]

Introduction

Critical infrastructures are essential to all of the necessary functions upon which society depends, but are largely taken for granted until those functions are disrupted. Events such as what took place at the Murrah Federal Building in Oklahoma City in 1994, preparation for Y2K (2000), 9/11 and its aftermath, the 2003 blackout of the northeast, and the devastating hurricanes of 2006 and 2008, all have focused attention on the nation's infrastructure, reminding us how vulnerable these systems are and the diversity of threats they face. As the American people have been confronted with the possibility of living and working without one or more of the basic necessities on which they have come to depend, critical infrastructure protection has become a priority for the federal government, as well as for the private sector and state, local, and tribal governments.

---

[1] For the Committee's other white papers, see: http://www.afcea.org/mission/intel/committee.asp#papers

[2] For more information on the Fall 2008 Symposium, see: http://www.afcea.org/events/fallintel/08/welcome.asp

It follows, therefore, that providing support to the critical infrastructure mission also has become an important priority for the U.S. Intelligence Community. Criticisms leveled against the Intelligence Community following 9/11 included concerns about the manner and extent to which foreign intelligence could be used to protect the homeland. In addition, the national debate about information and intelligence sharing now has been extended to include threats to the nation's critical infrastructure. Accompanying this discussion have been moves to build a more unified Intelligence Community (including the reorganization required by the Intelligence Reform and Terrorism Prevention Act of 2004) and more recent changes to Executive Order 12333. These changes allow for stronger support to state, local, and tribal authorities and to the private sector – in terms of technical assistance – and remove some impediments to sharing information with those charged with the critical infrastructure protection mission. These are important steps, but are not sufficient to providing intelligence support to the critical infrastructure protection mission.

Intelligence professionals and their customers share the view that intelligence is at its best when fully integrated with operations, such as when it provides direct support to those charged with taking action to prevent harm. Quality intelligence support therefore requires that the Intelligence Community not only understands the operations of the protectors of critical infrastructure, but also be integrated with those operations. With approximately 85% of the nation's critical infrastructure owned by the private sector, and no single, overarching body managing this infrastructure, providing and integrating this intelligence is a daunting task. It is all the more challenging because the Intelligence Community is not designed to provide intelligence support to groups other than governmental organizations. It is further complicated by the fact that fully seven years after the tragedy of 9/11, there is neither a consensus definition of domestic intelligence in public policy or in law, nor a framework that describes what domestic intelligence operations would be intended to achieve, particularly with regard to the critical infrastructure protection mission.

The critical infrastructure mission is described in a number of documents. For example, the National Response Framework (NRF), which in 2008 replaced the Federal Response Plan, describes a coordinated approach to domestic incident response. The Framework provides for a tiered response (federal, state, and local) to domestic emergencies, includes the National Incident Management System, and makes explicit provision for participation by the private sector and non-government organization (NGO) community. Similarly, the U.S. Department of Homeland Security has completed 17 Sector Support Plans (SSP) in support of the National Infrastructure Protection Plan (NIPP). The NIPP outlines a comprehensive risk management framework that defines critical infrastructure protection roles and responsibilities for all levels of government and private industry. In addition there are numerous organizations and initiatives that play a crucial role in supporting the critical infrastructure protection mission. Fusion centers facilitate information sharing across federal, state, local, and tribal governments. InfraGard, a public sector/private sector partnership, coordinates information sharing between the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), state and local law enforcement communities, the Intelligence Community, academia, and private sector members. A network of Information Sharing and Analysis Centers (ISACs) has been created to allow each critical infrastructure industry to communicate with its members, its government partners, and other ISACs about threat indications, vulnerabilities, and protective strategies. ISACs work together to better understand cross-industry dependencies and to account for them in emergency response planning.

These activities, documents and organizations are important, and could, taken together, form a framework for intelligence support to the Critical Infrastructure Protection Community. Building that framework requires that we begin to answer some fundamental questions.

- What makes an infrastructure critical? What sectors are critical?
- Does the infrastructure support a sector (e.g., banking), or does the infrastructure itself imply a sector (e.g., energy, communication, transportation)?

- Who owns the infrastructure to be protected? How do these owners make decisions on the protection of their infrastructure? How will they use intelligence to inform those decisions?
- How can intelligence requirements for critical infrastructure protection be defined? Who defines them? How can these requirements be made known to the Intelligence Community? How can the Intelligence Community share intelligence with those who own critical infrastructure?

The balance of this white paper addresses these questions and provides recommendations for operationalizing intelligence support to the Critical Infrastructure Protection Community. We focus particular attention on the role that existing organizations and processes can play to couple the intelligence needs of the nation's critical infrastructure with the capabilities of the Intelligence Community. We recognize that this paper's recommendations are far from definitive. However, the AFCEA Intelligence Committee hopes they will stimulate additional discussion resulting in a comprehensive approach to meeting the intelligence needs associated with protecting our critical infrastructure.

Defining "Critical Infrastructure"

Critical infrastructures are the complex and highly interdependent systems, networks, and assets that provide the services essential in our daily life. More specifically, critical infrastructures are those people, things, or systems that must be operational throughout our society to make daily living and working possible. Not all infrastructures are critical and not all critical infrastructures have the same level of importance. If everything is critical, then nothing is critical.

DHS, working in partnership with the private sector and state, local and tribal governments, has identified 17 critical infrastructure and key resource sectors: Banking and Finance; Chemical; Commercial Facilities; Commercial Nuclear Reactors, Materials, and Waste; Dams; Defense Industrial Base; Drinking Water and Wastewater Treatment Systems; Emergency Services; Energy; Food and Agriculture; Government Facilities;

Information Technology; National Monuments and Icons; Postal and Shipping; Public Health and Healthcare; Telecommunications; and Transportation Systems. Protecting these sectors is a very important effort that could guide intelligence support to the critical infrastructure protection mission; however it lacks sufficient granularity to focus that intelligence support. Interoperability and interdependency within and across sectors is not described by DHS, nor is there provision made for the role that geography plays in the criticality of some infrastructures as compared to others.

It seems clear that critical infrastructures must be considered as both sectors unto themselves and as infrastructures which support other sectors. For example, if an electric substation is damaged and the electricity goes out, railroad operations are disrupted and the flow of area traffic is impacted, causing a decreased movement of commodities and potential complications for emergency services. The substation then, is an energy sector asset that must be protected, but also a key element of other sectors' infrastructures. Similarly, if a major port is closed and transportation from that port ceases, the cascading effects are widespread in terms of the nation's economy. The food and agriculture industry across the country may be affected by a lack of incoming supplies, causing a slow-down in agricultural trade activity. Therefore, protecting ports and ensuring their uninterrupted operation is vital to the operations of other sectors. Advances in technology and Supervisory Control and Data Acquisition (SCADA) systems have enhanced individual sector operations, but at the same time increased the interdependencies among them, thereby creating additional vulnerabilities. Such vulnerabilities and gaps in security must be fully understood if we are to provide quality intelligence support to those who perform the critical infrastructure mission.

To reach the necessary understanding of what constitutes critical infrastructure, we propose the broad application of a decision framework to assist all who support the critical infrastructure mission, including the Intelligence Community. The framework recognizes that the definition of critical infrastructure will be different within and across the sectors, and within specific geographical areas. It also accepts that it is impossible to protect all infrastructures and allows for a prioritization of scarce assets and resources

based on priorities. This framework, characterized as the questions below, is a critical first step in understanding how the Intelligence Community can mobilize resources to support this vital mission.

- **Identify Critical Infrastructures:** What must we protect?
- **Determine Threats:** What threatens the things we must protect?
- **Determine Vulnerabilities:** How are those things vulnerable?
- **Determine Risk:** What risk is there of disruption?
- **Take Countermeasures:** If risk of disruption is unacceptable, what action can be taken to mitigate or eliminate the vulnerability?

The application of the decision framework described above can begin to answer the question of what is truly critical infrastructure and focus intelligence support. In addition, it can create a better understanding of the relationships between the supporting and supported role of sectors. With knowledge gained from the analysis of what infrastructures to protect as critical and their vulnerabilities, we will gain a greater understanding of the interdependencies between certain infrastructures. We can then provide information that can assist in protecting them accordingly. Understanding that one asset may be more critical than another because of its relationship to other infrastructures and essential services is the key to defining critical infrastructure at sufficient granularity to drive intelligence support.

It appears that some of the work described above has already been done by DHS in partnership with the owners and protectors of the nation's critical infrastructure. It also seems clear that this work has not been exposed broadly to the Intelligence Community, perhaps because no single authority has been identified as responsible for doing so.

Doing so, however, is important to developing the intelligence requirements necessary to support critical infrastructure protection. We recommend that the DHS Under Secretary for Intelligence and Analysis (I&A) assume that role because of his unique position as a member of both the Critical Infrastructure Community and the Intelligence Community, similar to the role played by the Undersecretary of Defense for Intelligence (USDI) within the military. I&A should lead an Intelligence Community-wide effort to formulate the definition of critical infrastructure for the Intelligence Community consistent with that role.

Identifying the Decisions Makers

As indicated above, defining critical infrastructure is an essential step to ensuring the provision of intelligence support to that mission. Equally important is defining the customer set for critical infrastructure intelligence and understanding how they make decisions. Intelligence is at its best when it is fully integrated with those charged with making decisions to secure our nation. We have learned this over many years in support of the military, policy, diplomatic and law enforcement communities. We can apply those lessons to the Critical Infrastructure Protection Community, provided we understand what that community is, how it conducts its mission, and can integrate intelligence support into that mission.

The 17 Sector Specific Plans (SSP) recently completed by DHS could be a useful framework for identifying the customer sets, the key decisions they must make, and a high-level information architecture for critical infrastructure protection intelligence support. The SSPs were developed through a collaborative process involving the federal sector-specific agencies, private sector owners and operators, state, local, and tribal entities, and other security partners. SSP define roles and responsibilities, catalog existing security authorities, institutionalize already existing security partnerships, and establish the strategic objectives required to achieve a level of risk reduction appropriate to each individual sector. Each SPP also requires a sector-specific risk-reduction consultative

network to exchange best practices and facilitate rapid threat-based information sharing among the federal, state, local, tribal and private sectors. Strategic objectives include:

- Rapidly reconstituting critical assets, systems and networks after an incident
- Planning for emergencies and updating response plans
- Ensuring timely, relevant and accurate threat information sharing between the law enforcement and intelligence communities and key decision makers in the sector
- Educating stakeholders on infrastructure resiliency and risk management practices

In short, the SSP create at the critical infrastructure sector level a shared view of the threat, outline key objectives and roles and responsibilities for supporting prevention and mitigation efforts, and identify a network of authorities through which information will be shared. In the language of the Intelligence Community, the SSP identify the critical infrastructure protection decision makers, the strategic objectives that must be supported by intelligence, and the networks over which critical infrastructure intelligence will be shared.

The Committee recommends that the Intelligence Community use the SSP methodology to formulate the broad outlines of a doctrine for intelligence support to the national critical infrastructure protection mission. A similar approach then could be applied at regional and local levels, led by the State Directors of Homeland Security and Fusion Centers. With a clear understanding of the national, regional, and local doctrine for critical infrastructure protection, intelligence support operations could be fully integrated into that doctrine at each level in the manner that best suits unique local environments and in compliance with the law. We recommend as well that the DHS I&A, acting as the bridge between the Intelligence Community and the critical infrastructure protection mission community, would be the logical person to lead such an effort at the national level.

Critical Infrastructure and the Private Sector

Critical infrastructure protection must fully integrate the disciplines of law, policy, intelligence and technology for enhancing the security of the nation's infrastructure. Fully 85% of the nation's critical infrastructure is owned and operated by the private sector. Effective intelligence support to critical infrastructure therefore must be supported by policy and law that enable support by the Intelligence Community to the private sector. As indicated previously, more than seven years after the tragedy of 9/11, no consensus definition of domestic intelligence has been formulated in law or public policy. As a consequence, there is no policy or legal framework within which to lay out the goals and objectives for what Intelligence Community support to the Critical Infrastructure Community would be designed to achieve. In the preceding sections of this paper, we have made recommendations for constructing a business model that could drive intelligence support to critical infrastructure protection. The larger issue of law and public policy that will be necessary to operate that model is beyond the scope of this paper, but must be ultimately addressed - perhaps by the next Administration - to operationalize intelligence support to critical infrastructure protection. The private sector is a truly non-traditional Intelligence Community customer set and presents a range of challenges, including sharing proprietary and classified information.

An examination of efforts to share information *within* the Critical Infrastructure Community - including the private sector - may provide a useful framework within which to integrate Intelligence Community support while larger policy and legal issues are being resolved. Critical infrastructure protection information sharing *within* the private sector appears to be very well developed, thanks in large measure to the Information Sharing Analysis Centers (ISACs). There are ISACs for most of the 17 SSP, and they consider themselves a community. ISACs provide trusted, collaborative, information/intelligence sharing and analysis capability for critical infrastructure owners and operators. Through the ISACs, industry experts establish working relationships; build trust; share sensitive vulnerability, threat, and mitigation information; conduct

informed analysis; and collaborate with other sectors and governments in an organized manner. Some ISACs operate operations centers to provide situation awareness and incident response, and have mechanisms to protect sensitive information. The unifying vision of the ISAC Community is to save lives through joint efforts. This vision is remarkably similar to that of the Intelligence Community.

We believe, then, that private industry already has developed a comprehensive structure for intelligence support to critical infrastructure protection and an information sharing architecture. At the Fall 2008 AFCEA Intelligence Symposium, we witnessed some frustration from private industry panelists who stated that in their view, what is missing in this framework is a clearly identified federal "plug-in" point for that structure. Private industry not only has a substantial economic stake in protecting their investments and ensuring the continued operation of their systems against a range of catastrophic threats, they are also in the best position to understand and prioritize the threats and devise mitigation strategies. Intelligence support to critical infrastructure protection that is not in large measure driven by the private sector simply would not be credible. The ISACs can be the voice of the private sector in the development of that strategy and they clearly need to have a federal plug in point identified. We recommend that the DNI designate that lead entity for the Intelligence Community with due speed.

Intelligence Requirements

Wikipedia defines an intelligence requirement as: "…an intelligence need that is specified by a decision maker, who passes the request to an intelligence agency, where an answer is developed and then disseminated. The formulation, setting, and evaluation of intelligence requirements are important elements of the intelligence cycle." Intelligence requirements, then, express the information needs of the decision makers and drive the priorities for Intelligence Community operations. At present we can identify no formalized mechanism for articulating intelligence requirements for critical infrastructure protection that includes the private sector, as well as state, local, and tribal governments: the decision makers for the critical infrastructure protection mission.

The lack of such a requirements process is understandable: this is a very complex issue. For example, it is clear that industry may benefit from intelligence information regarding threats from hostile foreign powers or their agents. It is less clear what information from the private sector would be of use to the larger federal efforts - including those of the Intelligence Community - to protect critical infrastructure. Still, for the private sector to assess information and respond to the government, the government must clearly articulate its priorities and its requirements for information. Similarly, the private sector must make its informational needs clear to the federal government, specifically to the Intelligence Community.

How then, might we move forward to create a requirements mechanism for intelligence support to critical infrastructure that includes the mission decision makers? We believe the building blocks are already there. The Intelligence Community has a long-functioning intelligence requirements process led by the DNI and validated by the National and Homeland Security Councils who represent the needs of the national security decision makers. That process begins with the President's articulation of national security issues. The DNI applies these issues to a National Intelligence Priorities Framework (NIPF) that serves as a high-level articulation of intelligence needs and priorities—essentially the operational orders for the Intelligence Community. The NIPF in its present form at least includes some components of the critical infrastructure protection mission. Each member of the Intelligence Community then translates the NIPF into specific collection, processing and analysis activities that respond to the needs articulated in the NIPF.

The critical infrastructure protection mission could easily be made a part of the larger NIPF process, for example as an unclassified annex. We recommend that the DHS I&A lead the critical infrastructure protection intelligence requirements process, consistent with his responsibility as articulated by both the Homeland Security Act of 2002 and the IRTPA. This process must be driven by the critical infrastructure protection decision makers. We recognize that this is a very diverse set of actors. We recommend that DHS I&A begin the process with the state homeland security directors and the ISAC directors.

Over time, the list of decision makers can be refined based on lessons learned in developing and promulgating intelligence requirements to support the critical infrastructure protection mission.

Conclusion

Before 9/11, the Intelligence Community focused on foreign threats. The Community's interaction with state, local and tribal law enforcement and other first responders intentionally was limited or non-existent. But homeland security, in a post-9/11 world, requires a new paradigm for intelligence support. It requires a network of state, local, federal, and private sector authorities working together to achieve a common goal: national protection. That network must be fully integrated into the traditional Intelligence Community as well as with new and essential partners at all levels of government and the private sector.

The creation of such a network is no small task. Much has already been put in place in support of its creation and we applaud those important and difficult accomplishments. Many things are working well, but more work is required. Our paper provides ideas and recommendations for moving this critical work forward. We hope it contributes in some measure to advancing intelligence support to critical infrastructure. The security of our nation demands it.