THE INTELLIGENCE COMMUNITY
NEW CHALLENGES, SOURCES, AND METHODS

A White Paper prepared by the AFCEA Intelligence Committee

October 2009




AFCEA

Serving Intelligence Professionals and their Community

The Intelligence Community:
New Challenges, Sources and Methods

Table of Contents

Introduction

The Intelligence Committee (the Committee) of the Armed Forces Communications and Electronics Association (AFCEA) is pleased to present this white paper focused on the changing threats facing our nation and the U.S. Intelligence Community (IC) and the potential represented by a wider variety of sources and analytic methodologies available to meet these threats. This paper is part of a series of Committee publications[1] intended to contribute to the ongoing national dialog regarding the state and future of the IC. The papers are intended to stimulate discussion at intelligence symposia presented by the Committee, and this one is keyed to the AFCEA Fall Intelligence Symposium scheduled for October 14 and 15, 2009.[2] Through the symposium and white paper, the Committee hopes to contribute to efforts to modulate the spectrum of threats with which the IC concerns itself and the sources and analytic approaches the Community employs to meet those challenges.

A Changing World of Threats and Challenges

The overview to the Fall Intelligence Symposium provides a succinct view of the new threat environment:

> The last year has seen a confluence of events which have produced arguably the largest change in the U.S. world view and intelligence priorities since the end of the Cold War. In congressional testimony, DNI [Director of National Intelligence] Dennis Blair singled out the economic downturn as "the primary near-term security concern" for the country, exacerbating traditional threats and producing new areas of instability around the globe. The operational and resource demands of the continuing wars in Iraq and Afghanistan have significantly, and perhaps fundamentally, altered the view of how the U.S. applies national power and of the force structure required. Additionally, the long-anticipated threat of cyber war appears to be showing signs of reality, with demonstrations in Estonia, Georgia and Iran and warnings of penetrations of some critical U.S. systems.

1 For previous white papers, see http://www.afcea.org/mission/intel/resource.asp#white.
2 See http://www.afcea.org/events/fallintel/09/welcome.asp.

The Committee views emerging threats like these and others as existing alongside more traditional intelligence challenges (e.g., the threat of proliferation of weapons of mass destruction or concerns regarding the effects of climate change on U.S. national interests).

Not only is the variety of threats expanding, but so is the nature of the threats. For example, the spread of a global information infrastructure will have long-term and profound effects on the international system. Historically, practitioners of international politics have had certain expectations regarding the behavior of nation states. These expectations have reflected both rules commonly observed by state governments as well as a common understanding of the prerogatives that obtain to governments.

Given the changing international security environment, these expectations are being called into question. For example:

- Is modern information technology—and the global information infrastructure it enables—changing what we can expect of actors in the international political system?
- Does it give these new actors prerogatives accorded traditionally to sovereign governments and, if so, is it doing so at the expense of those governments?
- Does communication technology pose new issues of policy and international security with which our government needs to be concerned?
- What must the IC do to help our government understand this issue's implications?

Cyber represents another important and recognized challenge facing the IC. Some commentators believe that cyberattacks (computer network attacks) can cause wide-scale disruptions to our nation's ability to sustain its critical infrastructure, the sovereign operations of its government and its ability to prosecute military operations. The cyber threat is particularly vexing in that it places at risk critical infrastructures owned and operated by the private sector for which a national interest exists. The government itself is seeking to build a secure cyber environment for both the public and private sectors.

Its influence over the private sector involves a complex mix of programs, regulatory initiatives and evolving industrial policy. These efforts must be informed by a solid understanding of adversary cyber capabilities and intentions.

Making the cyber threat more complicated are the low "barriers to entry" in that domain. While development and production of major conventional weapons and weapons of mass destruction and the development and sustainment of standing military forces requires a substantial resource base and organization, cyber operations fall within the capability of smaller, less well-resourced actors. Indeed, the principal barriers for entry for cyber—access to sophisticated information technology and broadband connectivity—have been largely surmounted. The 2006 war between Israel and Hezbollah found the latter equipped with a fiber optic backbone operating within one kilometer north of the Israel-Lebanon border. Cyberattacks and exploitation represent a potential threat ubiquitous in the hands of states, nonstate actors and individuals.

How should the IC respond to the cyber challenge, now and in the long term? For example:

- What is the changing mix of cyber capabilities available to real and potential adversaries?
- How do we determine adversary cyber intentions?
- How do we detect adversary cyber plans?
- What are our adversaries doing to develop cyber capabilities we have yet to suspect?
- How do adversary cyber operations threaten the Community itself?
- What intelligence requirements exist for cyber?
- What analytic cyber skills does the Community require? Where and how does it obtain those skills?

To be clear, cyber represents a difficult mix of challenges. The IC has work to do in overcoming existing deficits; it also needs to constitute an enduring capability to understand and anticipate cyber developments worldwide and their effects on our national interests. Indeed, the Community needs to

understand the changing national interests of our nation in regard to cyber on a global scale. This understanding represents a broad range of knowledge in politics, economics, technology, military affairs and even sociology. One aspect of cyber—cybercrime—represents a vital and dangerous link between the global economic crisis and growing cyber capabilities in the hands of adversaries and cybercriminals.

The global economic crisis to which the DNI referred provides another salient example of an area in which Community capabilities may be overmatched. The crisis itself provides numerous examples of questions with which the government must contend and for which intelligence is important. For example:

- To what extent is U.S. relative power affected by the crisis? How is the relative power of other states affected?
- What U.S. national interests are affected by the crisis, and how?
- How are our relations with allies, adversaries and other countries affected by actions we are taking or may take?
- What long-term changes in the international economic system are likely to occur?

Focus on the current economic crisis may prove short lived, but it should not be. Some commentators believe the recovery will result in long-term structural changes affecting the nature of U.S. employment. Others believe the recovery will be characterized by a hollowing out of U.S. manufacturing, with an even more significant shift of the U.S. economy toward services and increased U.S. dependence on foreign manufacturing of critical technologies. If they occur, these effects will modulate U.S. military, political and economic prospects in the world in addition to the well-being of our citizens. The Community has little choice but to master the global forces shaping these issues, both in support of current actions to combat the crisis and to equip decision makers with the tools necessary to position our nation successfully in the future global economy.

Another emerging issue, one already recognized by the Community's leadership, is global climate change. While debate continues regarding the scope of this challenge, many countries are taking actions that reflect their belief that global climate change is real and that it has an effect on their interests. Some countries are seeking to limit their carbon footprints; support is growing for international treaty obligations regarding carbon emissions. Some countries, such as Germany, appear to be seeking to gain competitive economic advantage by mastering "green" technologies that can reduce the effects of industry on the environment. Here again the Community is faced with a number of potential questions. Among them:

- Is U.S. global leadership enhanced or threatened by development of forward-leaning policies regarding global climate change?
- How is the United States perceived throughout the world regarding global climate change?
- Do we view the research and actions taken by other countries as corroborative to global climate change hypotheses?
- Can the United States gain competitive economic advantage through the development of specific technologies that can reduce environmental costs?
- If alternative energy approaches are required to deal with climate change, what are the implications for U.S. interests?

While the scope of the challenges faced by the Community has widened to an unprecedented extent, the dynamic nature of these changes represents a challenge itself. As a result, the traditional, topic-sensitive specialization of the Community must be accompanied today by the capacity to adopt a changing set of topics for collection, analysis and customer support. Indeed, implicit in the mission-manager approach taken by the Office of the Director of National Intelligence (ODNI) is the need to constitute mission and analytic teams flexibly, in response to a changing set of issues of concern. The Committee does not see, however, that the flexibility made possible by the mission-manager approach has come to fruition. The mission-manager set appears more static than the dynamic global environment suggests it should be.

Widening Our Sources

While considering these significant challenges in the threat environment, the Community also should look at the potential represented by new—or, perhaps more accurately, changing—sources, many of these "open source" in nature. The Argus capability, providing foreign bio-surveillance, represents a step in this direction, and we encourage the use of other tools to collect and analyze discipline-specific information useful to decision makers. At the same time, the Committee does not discount the need for secret intelligence. Indeed, our decision makers likely will continue to depend greatly on the information gained from sources that work deliberately to deny our access to that information, particularly as it relates to U.S. interests. Even if such information also is available openly, the fact that others seek to guard it should not be dismissed.

More challenging is that today's complex environment makes more difficult the act of keeping secret information out of the hands of the public and other governments. Further, some issues are shaped largely in public, with information that originates in the public domain. The creation of a global information infrastructure, the rise of social media and the cheap and almost ubiquitous access to advanced information technology diminishes the ability of governments to control information. For example, the 1986 Chernobyl incident challenged the Soviet government's ability to impose tight information controls. High-resolution, commercial satellite imagery made available through SPOT[3] revealed to the world the extent of the crisis, even as Soviet authorities sought to spin a different story. The 2003 SARS crisis in China marks another example of a government attempting—and failing—to control access to information. In this instance, global access to information conveyed through the Internet in general, and through social media in particular, represented an information equalizer between the Chinese authorities, the Chinese people and the rest of the world.

The recent disputed Iranian election offers a further example of a government seeking (but failing) to

3 System Probetoire d'Observation de la Terre.

dominate the information space. The Iranian regime tried to manage public discontent alternatively by shutting down social networking sites and then allowing the sites to function. Their efforts were largely unsuccessful because they could not manage the pace of change they faced.

These examples convey two broad implications for the IC. First, governments are finding it difficult to control the information they sought in the past to keep secret. Information technology in the hands of the public and nonstate actors, and the linking of government and public information infrastructures, means that more information is available through open source challenges. Second, matters important to the IC and its consumers are increasingly conducted in public. The rise of a global information infrastructure and social media has fundamentally altered the trajectory of these issues.

This changing global environment means that the Community must move well beyond open source in its relationship to foreign media. The IC has looked to foreign media for ways of gauging foreign capabilities and intentions, largely as a complement to its efforts to obtain secret intelligence. The Community should give strong and sustained emphasis to building an open source capability that captures both aspects of the global information environment—the availability of information that governments seek to restrict and the role information plays in changing the course and outcome of events. Important to this effort should be a combination of collection and analysis, in contrast to the traditional use of open source information as one component among others contributing to all-source analysis. While open source information can and should be used in that manner, it also should be viewed today as a component of the events themselves. In fact, some events (e.g., the Iranian political situation and China's response to the SARS crisis) cannot be understood properly without taking into account the role of information generated, disseminated and changed through the use of public channels.

Building Enduring and Agile Analytic Capabilities

The examples above also reflect the need to study societies and long-term trends. As a result, the

Committee echoes the call made by other commentators to rebuild deep, long-term capabilities in intelligence analysis. The Committee does not dismiss the need for "actionable intelligence" keyed to current geographic and country-specific issues and responsive to the needs of today's operational warfighters and diplomats. Even these issues, however, exist in context; societies can create social movements that challenge governments, and power can shift away from governments and into the hands of activists and nonstate actors. These intelligence issues require the same kind of resource-intensive and sustained commitment that more traditional strategic issues enjoyed. Our understanding of the global economy or telecommunications network, for example, must be no less nuanced and informed than was our understanding of the Soviet Union. The Community should regain its capacity in research and analysis to build long-term expertise and understanding of nations, movements and other topics of enduring concern.

New analytic techniques should accompany the widening spectrum of threats and challenges, just as they should accompany a sustained effort to regain the Community's strategic capacity. The dynamic relationships that exist between the global information infrastructure, critical infrastructure, the global economy, social movements and nonstate actors may require new approaches to modeling and simulation, approaches capable of taking into account a wider variety of factors and approaches that are able to uncover and evaluate subtle connections between factors. The Community may be able to study more intently and gauge more accurately both the capabilities and intentions of real and potential adversaries and regional and global competitors using new analytic approaches and tradecraft to uncover patterns of behavior in states and societies.

Prior Committee white papers[4,5] called for new and agile analytic techniques and structures. Indeed, the analytic flexibility for which the Committee called in these papers is more important than ever. While we will still seek to know quantitative measures of our adversaries' capabilities, we also need to

4 See "Making Analysis Relevant: It's More Than Connecting the Dots," AFCEA Intelligence Committee, Spring 2005 (http://www.afcea.org/mission/intel/documents/finalanalysiswp.pdf)

5 See "Enabling a Responsive and Agile Intelligence Enterprise," AFCEA Intelligence Committee, Spring 2008 (http://www.afcea.org/mission/intel/documents/SprinIntel08WP.pdf)

understand more subjective indicators of foreign political and social events. Such analysis would benefit from the sort of competitive approach for which the Committee called in 2005, an approach advocated by other commentators as well. The IC has made strides in information sharing; it now needs to gain ground in distributing the analytic effort, a recommendation the Committee also made in 2005. Distributed analysis offers the potential to form more competitive hypotheses, expose these hypotheses to a wider range of data and subject them to more thorough peer review. The combination of A-Space and Intellipedia provides an excellent mechanism that enables distributed analysis with diversity of analytic thought; their use should be encouraged and participation widened to include as many analysts as possible.

The Committee's spring 2008 white paper went further in proposing a flexible, topic-oriented approach to analysis. This approach goes beyond today's mission-manager approach, focusing on a fairly stable set of issues to allow for the formation and subsequent disestablishment of cells constituted for specific topics. Such cells, operating on a foundation layer of collaborative information infrastructure, would allow the Community swiftly to build teams with expertise necessary to address emerging challenges without changing the overall allocation of resources throughout the Community. This approach employs the Community's leadership as an “orchestration layer,” setting priorities, monitoring resources, and employing business intelligence to remain aware of the Community's efforts. The 2008 white paper looked to the RASER analytic efforts as one set of prototypes for the intelligence cells the Committee believes would make more agile our national intelligence analytic capabilities.

We view all these efforts as complementary. The agility and approach described by the Committee would provide flexibility to address current and emerging issues while generating additional intellectual capital useful for sustained intelligence research. A renewed commitment to analytic research would provide the rich contextual environment necessary to understand the global environment in which new issues emerge, making even more rewarding the agile approach described above. Both are needed.

Summary

The changing global environment represents many challenges to our nation. Some of these challenges are already evident; some will become apparent. Some will require better access to secret information; most will present themselves in both secret and public information generated through the use of social media and other aspects of the global information environment and infrastructure. The IC's approach to open source must take into account the need to gain information that corroborates classified information; it also must allow us to understand the role of public information in the trajectory and outcome of important issues.

In the past, the IC has demonstrated its ability to meet challenges no less significant than these. Its open source capabilities can be extended to meet the challenges of events shaped in large part by public information. The Community built—and can rebuild—sound intelligence analysis and research capabilities. Work sponsored by the ODNI has built the foundations of information sharing and collaboration. Bringing these capabilities together is necessary if the IC is to provide the intelligence support necessary to help our leaders make decisions about the changing global environment.

It is also entirely possible.