

Reflections on Intelligence Support to Cyber Operations

April 13, 2008

A White Paper

provided by



**This paper contains proprietary information that is intended solely for the US Government.
Disclosure to commercial companies or non-governmental organizations should be
coordinated with Innovative Analytics & Training, LLC.**

Innovative Analytics & Training, LLC
1050 Connecticut Ave, NW 10th Floor, Washington, DC 20036
<http://www.innovative-analytics.com> | 202-280-2045

Intelligence Support to Cyber Operations

by John E. Brennan

Introduction. We have entered a new conflict. The interconnectedness and resulting fragility of the United States is exposed and accessible in the cyber dimension of conflict. The fight is already underway.

What will the United States need? Cyber is a mission, not an –INT. It is a mission that will involve the talents, investment, and leadership of the government at all jurisdictional levels, industry, academia, science, and our international partners. Intelligence support – especially analysis – will be an important component to the cyber mission. This paper outlines some of the initial issues defense intelligence leaders should consider during this formative period – a period of increased investment in and attention to the cyber mission.

Issues and Considerations. The list below considers cyber from a number of operational and management issues. These issues include: missions, analysis, training and doctrine, research and development, and leadership. Each issue is briefly discussed and then augmented with a few ideas on how to further explore the issue area.

Missions. The cyber targets are diverse and range from large scale national-level missions (e.g., China) to small, sophisticated individuals or networks leveraging the technology of unwitting organizations around the world. The motivations are equally diverse and include asymmetric national defense capabilities, theft of intellectual property, theft of money and resources, curiosity, and notoriety or prestige. Estimating the size, capabilities, motivations, and intentions of these targets should be a central focus of defense intelligence. Mission considerations:

1. Basic research across open and US sources to define a gross picture of the targets will help inform where and how to apply defense intelligence analytic resources.
2. Defining a spectrum of malicious cyber activities (sophisticated national attack, identity theft to fund terrorism or illicit trafficking operations, cyber vandalism) and their potential first and second order impacts to US national interests will help defense intelligence understand the severity or priority model necessary to allocate analytic resources.

Analysis. US defense intelligence leaders should deliberately design the analytic efforts necessary to inform and support US cyber activities. The potential for laying the wrong foundation is very real. Equally real is the potential to devolve into a bureaucratic struggle over

definitions, responsibilities, and resources at a time when the adversaries have already organized and are conducting operations. Being deliberate does not mean going slow. However, it does mean having a defined approach for experimentation with different organizational and analytic models, not simply repeating what has been used in other intelligence missions. Certainly some of the research activities described in the *Mission* section can inform the formation of analytic capabilities, but there may be a need to “take stock” of current US cyber operational and analytic efforts. Analysis considerations:

1. Defining and understanding the US cyber operational capabilities and strategies for covert action, open offense, and open defense will help defense intelligence analytic leaders begin to understand the types of intelligence support required (strategic intelligence, monitoring, tactical warning, targeting, etc.). This knowledge can lead to an analytic program including the customer needs, missions, analytic strategies, assignments, reporting lines, and collection strategies across all intelligence collection programs. A Cyber Analysis Advisory Group (CAAG, pronounced cage) can help bring critical attention and additional due diligence to this issue.
2. With an understanding of the cyber missions and analytic needs, defense intelligence leaders can then begin to craft a new analytic discipline focused on cyber. Defining an analytic development framework from initial entry to the senior ranks can help inform the hiring and training needs for defense intelligence analysis. The competition for analysts and talent in this space will be fierce for many years to come. It will be important to organize an initial cadre of analysts who can guide the formation of this discipline. It may parallel the experience in creating sonar or radar analysts during the early formation of those disciplines. A historical review of that experience could inform this new activity. The goal is to avoid the identity crisis and internecine fights many GEOINT analysts were plagued with. If the formation of US air, special, and joint forces are any indicator, it will be difficult to avoid the “turf battles” over creating our cyber forces.

Training and Doctrine. The military services and the Department of Defense have the processes and capabilities necessary to scale to meet the training and doctrine needs of the US cyber mission. These activities must be informed by the current and projected outlook of foreign cyber actions. This initial picture will inform the training of cyber analysts for a generation. The training of cyber analysts will be complex, blending: mathematics, computer and network operations at the software and hardware component level, computer forensics, general military theory, critical infrastructure/industry knowledge, offensive and defensive operations, strategic

intelligence, and understanding of foreign information technology practices among other diverse knowledge and skills. Training and Doctrine considerations:

1. Defense intelligence leaders should undertake a study of adversary training and doctrine. This information may inform the formation of US capabilities.
2. Defense intelligence leaders should undertake a survey of the best analytic practices across existing cyber, information operations, computer network operations, and C4ISR analytic organizations. The focus should be on identifying strategic, operation, and tactical intelligence practices, procedures, methods, and analyst traits to bolster and expand.
3. Defense intelligence should develop and launch an orientation class to teach and open a dialog with customers and policy makers on what to expect from intelligence support to cyber.

Research and Development. Cold War II is a struggle between technologists. Research and development will be the foundation for winning the struggle. The “weapons systems” for Cold War II will be produced and “fielded” in hours or days, not years or decades. Therefore, cyber intelligence analysis must view R&D as an operational activity – an integral component of analysis, not an add-on or separate organization. The fact that this section of the paper is separate from the analysis section underscores the difficulty in overcoming the R&D stereotype. Research and Development considerations:

1. Defense intelligence leaders should develop a deliberate strategy for cyber analytic test-beds within the emerging intelligence organizations focused on cyber.
2. Defense intelligence leaders should organize a future needs group to define, guide, and coordinate the portfolio of research and development activities assigned to each intelligence analysis organization.

Leadership. Forming the nation’s cyber intelligence capabilities is akin to forming the initial leadership teams of the US nuclear forces. US defense intelligence leaders should develop a rigorous approach to organizing and selecting the initial leadership cadre. This leadership team should be organized jointly with US national intelligence leaders. Leadership considerations:

1. Defense intelligence leaders should recommend the creation of a National Intelligence Officer (NIO) and staff for Cyber. The NIO could have a combination of functionally- and organizationally-focused deputies, including deputies for nation-states, non-state actors, government infrastructure, and commercial infrastructure.

Summary. Cyber capabilities present state and non-state actors with asymmetric and plausibly deniable options. When directed at US economic and infrastructure interests they can potentially multiply and extend the effects. Foreign cyber activity is migrating from disjointed, small-scale, exploratory efforts to deliberate, systematic efforts. The risks and the potential effects will continue to grow as more and more economic, communications, and general human activity moves online. A general, persistent cyber cold war will continue for the foreseeable future. US defense intelligence leaders have an opportunity to design the intelligence analytic capabilities that will inform and secure US cyber interests and capabilities. The issues of mission, analysis (including R&D), training and doctrine, and leadership should remain a focus of defense intelligence leaders for the coming year.