DoD Global Information Grid Mission Assurance

Anthony Bargar
OASD/NII, DASD(IIA)

The DoD's policy, planning, and warfighting capabilities are heavily dependent on the IT foundation provided by the GIG. However, the GIG was built for business efficiency instead of mission assurance against sophisticated adversaries who have demonstrated intent and proven their ability to use cyber as a tool for espionage and the criminal theft of data. GIG mission assurance works to ensure the DoD is able to accomplish its critical missions when networks, services, or information are unavailable, degraded, or distrusted. This article explores current threats to the GIG and outlines the solutions that the DoD has developed to protect our networks.

The information environment in which the DoD operates is global, mobile, and interconnected. Dependence on shared critical information infrastructures are a strategic advantage as well as a weakness. National security is challenged by sophisticated adversaries who have demonstrated intent and proven their ability to use cyber as a tool for espionage and the criminal theft of data. Successfully defending the DoD's networks and information from sophisticated adversaries is a serious challenge. Unlike the hacker community, sophisticated adversaries are well resourced, trained, and often have the backing of foreign intelligence services, transnational groups, or organized crime. Sophisticated adversaries leverage a full range of information operations to achieve their goals. Every year, attempts to penetrate DoD networks increase; still, there has been no wide-scale disruption of the critical information infrastructures on which the DoD depends for mission success.

However, in February 2008, the IC warned of increasing cyber attacks by foreign governments, non-state actors, and criminal elements exploiting vulnerabilities of the U.S. information infrastructure [1]. Sophisticated adversaries have the technical means, the insider knowledge of national infrastructures, and the intent to manipulate data and disrupt critical and vulnerable national resources. At the same time, the DoD Inspector General published an audit of the DoD's mission-critical IT systems which found that 61 percent lacked contingency plans or evidence of such plans, and 82 percent have never been exercised, leading the audit to conclude that " ... DoD mission-critical systems may not be able to sustain warfighter operations during a disruptive or catastrophic event" [2].

National security depends on assured global information infrastructures that are reliable and resilient. Real-time risk management and situational awareness are essential to responding to a cyber crisis, as is the consideration of what national security missions are affected, potential cascade effects, and the prioritized approaches for restoration.

National security depends on assured global information infrastructures that are reliable and resilient. Real-time risk management and situational awareness are essential to responding to a cyber crisis ...

The DoD's policy, planning, and warfighting capabilities are heavily dependent on the IT foundation provided by the GIG. Net-centric information environments provide reliable, instant, and meaningful information that shape DoD positions, as well as prepare and enable a joint warfighting force to dominate air, land, maritime, and space. In 2006, the DoD aligned cyberspace as a warfighting domain alongside the traditional domains of air, land, maritime, and space. However, it is not a sanctuary advantage for the DoD, but a borderless, pervasive, and hostile operating environment for all missions.

In February 2007, responding to growing threats to the GIG, the DoD took additional steps to increase resilience against sophisticated cyber attacks. DoD leadership recognized that the solution set included a broad spectrum of experts from IA, the Homeland Security Critical Infrastructure, and the Joint Chiefs of Staff. A working group was charged with analyzing the issue and laying out a plan of action to ensure that the DoD is able to accomplish its critical missions when networks, services, or information are unavailable, degraded, or untrusted. The DoD's mission-essential functions (MEFs) such as deploying the armed forces, maintaining command authority, and global situational awareness were deemed critical. GIG mission assurance was defined as *the level of confidence that the GIG will provide adequate support for critical MEFs in the face of full-spectrum attack from a sophisticated adversary*.

The scope of the problem includes the networks, services, and information needed to conduct cyberspace operations, consistent with the National Military Strategy for Cyberspace Operations and other documents such as the National Strategy to Secure Cyberspace [3] and the National Response Framework [4]. Additionally, to improve resiliency, protection, and continuity of services, the underlying infrastructures such as power and telecommunications networks are critical to the DoD's ability to conduct its missions. Guiding principals for the initiative include the following:

- GIG mission assurance is a continuously changing and adapting set of capabilities protecting against all adversaries which ensures execution of mission essential functions.
- GIG mission assurance is built on survivable communications (transport),

trustable information (content), and timely services (applications).

- Mission operations (the warfighter) must allow for and compensate for failures and losses from natural and human adversaries that are persistently present.
- The GIG must provide force-wide survivable, robust, and resilient capabilities against sophisticated adversaries.

The problem domain is large and spans people, processes, technology, associated training, policy/governance, and architectures. There are many disciplines and organizations involved within the DoD including, but not limited to, cyber protection, detection, reconstitution, intelligence, continuity of operations, and critical infrastructure protection. Additionally, the DoD's role in national response, emergency preparedness, and support must be considered in a holistic approach for addressing how the GIG enables essential missions. Ensuring the DoD can accomplish these missions while operating in a degraded information environment requires a much broader range of activities, and requires close coordination between the IT community and the warfighter. For example, to accomplish the MEFs, the warfighter must define more concise technology requirements as well as train and equip forces to achieve mission success despite a degraded cyber domain. Additionally, the IT community must provide the warfighter situational awareness for failure and cascade effects of the GIG as related to specific MEFs, and build diverse and resilient capabilities. During a sophisticated attack, the IT community must restore capabilities to support current mission priorities as the warfighter compensates for loss in services. In short, the DoD's response activities must operate at *the speed of light, verses the speed of policy*. Response options must be synchronized, prioritized, and coordinated to minimize effects on national security missions and ensure that MEFs can successfully survive an attack.

Conclusion and 2008 Priorities

In a net-centric information environment that is globally interconnected, there are insufficient resources to protect and defend all aspects of the GIG at all times from growing and asymmetric threats. Additionally, the DoD GIG can be denied or degraded by non-cyber events on dependent critical infrastructures such as power and telecommunications. A change in philosophy is needed, as well as an integrating framework for a holistic approach balancing resources and risk to protect our capabilities which enable MEFs. There are steps both strategic and actionable to improve the DoD's posture and ability to survive sophisticated cyberspace attacks. GIG support to mission assurance requires integrated plans, programs, and operations across IA, computer network defense, cyberspace intelligence activities, and critical infrastructure protection. To better understand the shortfalls and enable solutions, DoD priorities in this area include the following:

- Exercising military operations under a severely degraded cyber environment.
- Improving resilience, prioritization for recovery, and continuity of operations.
- Redefining network command and control capabilities with regard to prioritized reconstitution of GIG services.
- Resourcing and planning for mission assurance with combatant commands, services, and agencies.

The bottom line is that the GIG is DoD s force multiplier for mission success in air, land, sea, and cyberspace ...The DoD is acting on the solutions necessary to ensure mission success.

The bottom line is that the GIG is the DoD's force multiplier for mission success in air, land, sea, and cyberspace. The GIG must compensate for loss due to cyberspace disruption, and the users must prepare to operate in a degraded environment. The DoD is acting on the solutions necessary to ensure mission success.◆

References

1. "Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence." 5 Feb. 2008 <www.dni.gov/testimonies/20080205_transcript.pdf>.
2. Office of the Deputy Inspector General. "Contingency Planning for DoD Mission-Critical Information Systems." 5 Feb. 2008 <www.dodig.osd.mil/Audit/reports/fy08/08-047.pdf>.
3. "National Strategy to Secure Cyberspace." Feb. 2003 <www.whitehouse.gov/pcipb>.
4. Department of Homeland Security. "National Response Framework." Jan. 2008 <www.fema.gov/pdf/emergency/nrf/nrf-core.pdf>.

About the Author

Anthony Bargar is a senior policy analyst leading DoD's GIG mission assurance for the DASD(IIA) where he leads the strategic goal to transform and enable IA capabilities for the DoD and supports the DoD's IA responsibilities in the interagency critical infrastructure protection programs. Previously, he served as IA-Senior Technology Advisor for the Counterintelligence Field Activity, and Senior IA Analyst for the Defense Intelligence Agency, where he implemented the Defense Intelligence Communities Enterprise Risk Management System. Bargar led a research project for the DoD on shared critical information infrastructure protection and defense with the National Defense University (NDU) and the Swedish National Defense College. He holds a master's degree in information and telecommunication systems for business from Johns Hopkins University. Additionally, he is a distinguished graduate from the NDU Information Resources Management College.

E-mail: anthony.bargar@osd.mil

Acronym Key for This Issue

AIS:	Assured Information Sharing
C&A:	Certification and Accreditation
CIO:	Chief Information Officer
CNSS:	Committee on National Security Systems
DASD(IIA):	Deputy Assistant Secretary of Defense for Information and Identity Assurance
DIACAP:	DoD Information Assurance Certification and Accreditation Process
DIAP:	Defense Information Assurance Program
DISA:	Defense Information Systems Agency
DNI:	Director of National Intelligence
DoD:	Department of Defense
GIAP:	GIG IA Portfolio (Management)
GIG:	Global Information Grid
IA:	Information Assurance
IC:	Intelligence Community
INFOSEC:	Information Security
IT:	Information Technology
NII:	Networks and Information Integration
NSA:	National Security Agency
NSS:	National Security Strategy
R&D:	Research and Development
SME:	Subject Matter Expert
UCDMO:	Unified Cross Domain Management Office
USG:	United States Government