Order Code RS21590
Updated March 11, 2005

Defense Program Issue: Global Information Grid, Bandwidth Expansion (GIG-BE)

Clay Wilson
Specialist in Technology and National Security
Foreign Affairs, Defense, and Trade Division

Summary

The Global Information Grid (GIG) is the enabling infrastructure for Network Centric Warfare (NCW), a concept that relies on communications technology to link together U.S. military personnel, ground vehicles, aircraft, and naval vessels through integrated wide and local area networks to provide improved battle space awareness for joint military forces.[1] The GIG Bandwidth Expansion program (GIG-BE) is a component of the overall GIG, that involves upgrading the capacity of the busiest equipment and transmission pathways composing the central portion of the GIG. Some question whether the GIG-BE design will support military requirements for transmitting the expected future high volume of encrypted network traffic. Also, because each service is developing a separate network architecture that will tie into the GIG, some observers question whether these differences will limit interoperability of the overall GIG, and thus reduce its usefulness to warfighters. This report will be updated as events warrant.

Background

Global Information Grid. DOD is building a Global Information Grid (GIG) to provide a secure networking capability for managing information on demand for warfighters, policy makers, and support personnel. The GIG will provide a single network to enable sharing of information from sensors among personnel at multiple levels of security in all services, in the intelligence community, and with U.S. coalition partners. The functionality of many sophisticated weapons systems may be critically dependent on the future capabilities of the GIG.

GIG-Bandwidth Expansion Program (GIG-BE). The GIG network design includes linkages through radio, satellite, and land lines. The GIG-BE program enhances the high-speed land lines which form a central core of the GIG, and which use optical network technology. The Defense Information Systems Agency (DISA) is leading the

[1] For more information about Network Centric Warfare, see CRS Report RS20557, *Navy Network-Centric Warfare Concept: Key Programs and Issues for Congress.*

two-year GIG-BE program which will link 100 top defense and intelligence sites across the globe through a new high-bandwidth, high-speed, 10 gigabits-per-second optical Internet Protocol Network, and is planning to deploy network upgrades for at least 90 "central point" sites by Fall 2005. The list of these "central point" sites is classified, but locations both in and outside the United States are included. Once the bandwidth expansion is deployed, the DISA will next improve user services for the GIG through its GIG Enterprise Services (GES) initiative.[2]

Bandwidth Needs. According to former Assistant Secretary of Defense for Networks and Information Integration (ASD/NII), John Stenbit, the primary problem that must be overcome to make information for NCW easily accessible through the GIG is meeting the demand for bandwidth.[3] Encryption requirements for high security for the GIG will add considerable management overhead signaling to all network traffic and will significantly reduce the amount of bandwidth that is actually available for conveying a message. By the year 2010, the Congressional Budget Office (CBO) estimates that the supply of effective bandwidth required by the Army will fall short of peak demand by a ratio of approximately 1 to 10.[4] Also, DISA reportedly has projected that requirements for transmission of all encrypted U.S. military information will grow by about 50 percent per year in the future. However, CBO has calculated that the existing design for the GIG-BE program, which supports the core of the GIG, is adequate to support military needs through 2015 and possibly through 2020, with technology upgrades.[5]

Network Architectures. The "architecture" of the GIG network includes the design to support business functions and military operations (the enterprise architecture), plus the design for transmission of data within each network (the technical architecture). Each military service is currently creating its own network architecture to support warfighters, and tie into the GIG. The key architectures are (a) the Air Force C2 Constellation, (b) Navy and Marine Corps ForceNet, and (c) Army LandWarNet. However, many observers are concerned that interoperability problems between the different architectures used by each military service may limit the usefulness of the GIG, leaving warfighters unable to tap into all network capabilities.[6]

---

[2] Chris Watson and Tony Stout, "Net-Centric," *Government Computer News*, vol. 22, no. 30, Oct. 13, 2003.

[3] In certain situations during Operation Iraqi Freedom, commanders had access to only one communications channel. If someone else was using it first, the commander had to wait until it was free for him to use. Matthew French, "Bandwidth in Iraq a Subject of Debate," *Federal Computer Week*, Oct. 20, 2003, p. 43.

[4] Anticipated hardware improvements by 2010 will shift the existing bandwidth bottleneck from the brigade level to the corps level. If the Joint Tactical Radio System (JTRS) performs as the Army projects, the new radio may provide more than enough bandwidth for the lower tactical levels of command, with a margin for growth of demand beyond 2010. However, at the division and corps level, the projected demand is still expected to be much greater than the likely supply. CBO, *The Army's Bandwidth Bottleneck*, Aug. 2003 at [http://www.cbo.gov].

[5] CBO, *Issues Associated with the Global Information Grid Bandwidth Expansion*, Feb. 28, 2005, p. 15.

[6] *Implementation of the Interoperability and Information Assurance Policies for Acquisition of* (continued...)

Air Force C2 Constellation. The Air Force Multi-Sensor Command and Control Constellation (formerly MC2C), now known as the C2 Constellation program, consists of several technical and enterprise architectures, some of which are designed to relay information directly between machines using common information standards. The "constellation" consists of platforms, ground stations, unmanned aerial vehicles, space-based sensors, and possibly new multi-sensor command and control aircraft. The C2 Constellation will be one of many Air Force enterprise architectures that also support the business process for acquiring future C2 capabilities.[7] The enterprise architectures are coordinated by a group of Air Force Domain Councils that in turn are governed by the Enterprise Architecture Integration Council, which is an executive oversight board headed by John Gilligan, the Air Force CIO.[8] The C2 Constellation may also be described as an approach to program management for improving Air Force C4ISR capabilities.[9]

Navy and Marine Corps ForceNet. ForceNet is a concept for a communications network that combines all networks and business processes for Navy and Marine Corps systems, so that information can be gathered and analyzed in a collaborative, at-sea-environment. For example, naval strike group commanders can use computer network "chat rooms" to coordinate among their warfare commanders and ships, as well as reach back to the continental United States for help in diagnosing problems.[10] ForceNet maintains a continual state of evolution based on changes in technology and changes in the battle space, and is not intended to have an "end" state. As such, ForceNet is not a program or a system, but rather a way of integrating a wide array of technological resources into a distributed, networked combat force available in real time to all personnel.[11] It is an architecture comprised of networked systems, processing and computing, and interfaces that are secure and transparent to users.[12] Detailed information about the architecture for ForceNet can be found in CRS Report RS20557, *Navy Network-Centric Warfare Concept: Key Programs and Issues for Congress*.

---

[6] (...continued)
Navy Systems, DOD Inspector General, Report No. D-2005-003, Feb. 2, 2005; Government Accountability Office, *Defense Acquisitions: The Global Information Grid and Challenges Facing Its Implementation*, GAO-04-858; and Lisa Troshinsky, " DOD Has No Clear Strategy for GIG, GAO Says," *Aerospace Daily & Defense Report*, Aug. 2, 2004, p. 5.

[7] Hanscom Air Force Base, *"Constellation" Greater Than the Sum of Its Parts*, press release, Feb. 20, 2003 at [http://esc.hanscom.af.mil].

[8] Dawn S. Onley, "Air Force Working to Connect Sensors," *Government Computer News*, May 1, 2003 at [http://www.gcn.com].

[9] *"Constellation"* press release, Feb. 20, 2003, op.cit.

[10] Admiral Walter F. Doran, "ForceNet Deployer," *Military Information Technology*, Nov. 29, 2003 at [http://www.mit-kmi.com].

[11] Rear Admiral Thomas E. Zelibor, Statement to the House Committee on Armed Services, Subcommittee on Terrorism, Unconventional Threats and Capabilities, Feb. 11, 2004 and J.D. Walter, "ForceNet: Delivers Future Capabilities Now," *Flagship*, Dec. 11, 2003, [http://www.flagshipnews.com/].

[12] U. S. Naval Office of Information at [http://www.chinfo.navy.mil/navpalib/policy/vision/vis02/vpp02-ch3v.html].

Army LandWarNet. LandWarNet is the Army counterpart to the Air Force C2 Constellation and the enterprise network of the Navy's ForceNet, and enables connectivity to the GIG for the following systems: (1) National Guard's GuardNET; (2) the Army Reserve's ARNET; (3) Echelons-Above-Corps connectivity to the GIG supporting Combatant Commanders, Land Component Commanders, and Joint Force Commanders, and providing the bridge between the deployed soldier and the GIG; and (4) Echelons-Corps-and-Below connectivity to the GIG supporting soldiers, units of action/brigade, and Division and Corps elements located in the deployed theater. When fielded, the Warfighter Information Network-Tactical (WIN-T), Joint Tactical Radio System (JTRS), Transformational Communications System, and Network Centric Enterprise Services will be integral parts of LandWarNet, all linked to the GIG.[13]

Oversight Issues for Congress

The GIG-BE program raises several potential oversight issues for Congress.

Transmission Capacity of the GIG-BE. Is the current design for the GIG-BE sufficient to support future projections for the bandwidth requirements to properly secure classified military transmissions? Do reported projections for bandwidth requirements adequately take into account extending the functionality of the GIG down to each individual soldier, and to each individual sensor and individual weapons system in the future? Do the calculations for growth in GIG-BE transmission capacity adequately incorporate estimates for future changes in network technology, future developments in weapons design, and future military tactics?

Interoperability of GIG Architectures. Each military service is creating its own network architecture, causing many observers to be concerned that interoperability problems between the different architectures may limit the usefulness of the overall GIG, leaving warfighters unable to tap into all network capabilities.

DOD officials have reportedly stated that all services' network architectures are basically the same network, and that once the information systems are integrated, all military units will be able to access whatever data they need (policy and security features will control the level of access for each individual). DOD intends to integrate all the separate architectures using a plan known as the Joint Technical Architecture (JTA) and the Net Centric Operations and Warfare Reference Model (NCOWRM).[14] A new DOD requirements development process, known as the "Joint Capabilities Integration and Development System," now requires that all technology systems acquired to become part of the GIG must include joint operational capabilities as part of their development and

---

[13] "Army Renames Its Network Enterprise," Feb. 26, 2004 at [http://www.insidedefense.com/].

[14] Brigadier General Marc Rogers, Director Joint Requirements and Integration Directorate/ J8, for U.S. Joint Forces Command, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, hearing on Military C4I Systems, Oct. 21, 2003 at [http://www.cq.com]. Statement of John Stenbit, Assistant Secretary of Defense for Networks and Information Integration, House Committee on Armed Services, Subcommittee on Terrorism, Unconventional Threats, and Capabilities, Feb. 11, 2004.

delivery.[15] The DOD Joint Staff has also created a new Force Capability Board (FCB) to monitor NCW programs for mismatches in funding, or mismatches in capability.[16] The Defense Department is also merging its Business Systems Modernization (BSM) effort with its Global Information Grid architecture project to ensure that all network architecture efforts comply with GIG standards.[17]

However, some questions remain. To what degree are these DOD efforts to integrate differing network architectures proving effective? Are the immediate needs of the war in Iraq reinforcing the use of different network architectures? What are some possible vulnerabilities as the enterprise and technology architectures of the GIG network become more fully interoperable? Does increased interoperability also increase the potential for unauthorized access or "hacking" of the GIG? Under what circumstances might it be better to maintain a military communications network using architectures and technologies that are less homogeneous? As technology evolves for attacking networks, will security for the GIG be adequate to insure reliability of equipment and authenticity for users and data?

---

[15] Rich Tuttle, "New Organization to Stress Importance of Network Programs," *Aerospace Daily*, Jan. 30, 2004.

[16] Rich Tuttle, op. cit.

[17] Jason Miller, "DOD Builds on GIG Blueprint," *Government Computer News*, vol. 23, no. 1, Jan. 12, 2004.