

An hourglass-shaped graphic with a globe inside. The top bulb is dark blue, and the bottom bulb is light blue. The globe is centered in the narrow neck of the hourglass. The word "WikiLeaks" is written in white on a dark blue rectangular background at the bottom of the graphic.

# WikiLeaks Document Release

<http://wikileaks.org/wiki/CRS-RS21590>

February 2, 2009

Congressional Research Service

Report RS21590

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

Clay Wilson, Foreign Affairs, Defense, and Trade Division

March 11, 2005

**Abstract.** 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. 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.

WikiLeaks

# CRS Report for Congress

Received through the CRS Web

## 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.<sup>1</sup> The GIG Bandwidth Expansion program (GIG-BE) is a component of the overall GIG which upgrades the transmission pathways composing the central portion of the GIG. The GIG-BE program achieved full operational capability as of December 20, 2005, however, 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.** The DOD Global Information Grid (GIG) provides a secure networking capability for managing information on demand for warfighters, policy makers, and support personnel. The GIG is a single network that enables communications and sharing of sensor information 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 capabilities and reliability of the GIG.

**Status of the 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 by using optical network technology.

---

<sup>1</sup> For more information about Network Centric Warfare, see CRS Report RS20557, *Navy Network-Centric Warfare Concept: Key Programs and Issues for Congress*, by Ronald O'Rourke.

The Defense Information Systems Agency (DISA) announced that the GIG-BE program has completed operational testing and achieved full operational capability as of December 20, 2005. The GIG-BE is now accredited to support high-bandwidth, synchronous optical network transmission of classified data traffic at 10 gigabits-per-second between 86 “central point” defense sites, and may eventually extend to link 100 top defense and intelligence sites.<sup>2</sup> The list of “central point” sites is classified, but includes locations both inside and outside the United States.

**Future Plans for the GIG-BE.** Network transmissions for the Defense Information Systems Network (DISN) that now operate over leased lines will soon be integrated into the new GIG-BE transmission pathways which are owned by DOD.<sup>3</sup> The GIG-BE will eventually be linked with the Joint Tactical Radio System (JTRS) and the Transformational Communications Architecture to form a high-speed, high-capacity network. The Army is upgrading its LandWarNet networks to tie into the GIG-BE through its Installation Information Infrastructure Modernization Program (I3MP), the Air Force will tie all its bases into the GIG-BE through the Air Force Combat Information Transport System, and the Navy will connect with the GIG-BE through its FORCENet architecture.<sup>4</sup>

**Network Architectures.** The “architecture” of the GIG network includes the functional design to support business, logistics, intelligence sharing, and military operations (the enterprise architecture), plus the technical 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.<sup>5</sup>

---

<sup>2</sup> Jason Miller, “DOD’s GIG-BE reaches full operational capability”, *Government Computer News*, December 20, 2005, [[http://www.gcn.com/vol1\\_no1/daily-updates/37848-1.html](http://www.gcn.com/vol1_no1/daily-updates/37848-1.html)].

<sup>3</sup>

Dawn Onley, “GIG-BE Program director Montemarano gets new assignment”, *Government Computer News*, November 11, 2005, [[http://www.gcn.com/vol1\\_no1/daily-updates/37547-1.html](http://www.gcn.com/vol1_no1/daily-updates/37547-1.html)].

<sup>4</sup>

Dawn Onley, “Military services open the door to GIG-BE”, *Government Computer News*, November 11, 2004, [<http://appserv.gcn.com/cgi-bin/udt/im.display.printable?client.id=gcn2&story.id=27963>].

<sup>5</sup> *Implementation of the Interoperability and Information Assurance Policies for Acquisition of 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.

**Air Force C2 Constellation.** 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” platforms include ground stations, unmanned aerial vehicles, space-based sensors, and possibly new multi-sensor command and control aircraft. Within the C2 Constellation program, the Combat Information Transport System is designed to deliver operational information to warfighters.<sup>6</sup> The C2 Constellation will also support the business process for acquiring future C4ISR capabilities.<sup>7</sup> The architecture is coordinated by a group of Air Force Domain Councils that in turn are governed by the Enterprise Architecture Integration Council.<sup>8</sup>

**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.<sup>9</sup> 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.<sup>10</sup> It is an architecture comprised of networked systems, processing and computing, and interfaces that are secure and transparent to users.<sup>11</sup> A more detailed discussion of the architecture for ForceNet can be found in CRS Report RS20557, *Navy Network-Centric Warfare Concept: Key Programs and Issues for Congress*, by Ronald O’Rourke.

**Army LandWarNet.** The Installation Information Infrastructure Modernization Program (I3MP) is the installation portion of the Warfighter Information Network-Tactical (WIN-T) that supports training, mobilization, and logistics.<sup>12</sup> The Warfighter Information Network-Tactical, Joint Tactical Radio System (JTRS), Transformational

---

<sup>6</sup> Doug Beizer, The Air Force Patrols the Network, *Government Computer News*, August 15, 2005, Vol. 24, No. 3, [[http://www.gcn.com/24\\_23/dodcomputing/36618-1.html](http://www.gcn.com/24_23/dodcomputing/36618-1.html)].

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

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

<sup>9</sup> Admiral Walter F. Doran, “ForceNet Deployer,” *Military Information Technology*, Nov. 29, 2003 at [<http://www.mit-kmi.com>].

<sup>10</sup> 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/>].

<sup>11</sup> U. S. Naval Office of Information at [<http://www.chinfo.navy.mil/navpalib/policy/vision/vis02/vpp02-ch3v.html>].

<sup>12</sup>

Army Directorate of Information Management, [[http://www.doim.army.mil/I3MP\\_Program.html](http://www.doim.army.mil/I3MP_Program.html)].

Communications Architecture, and Network Centric Enterprise Services are integral parts of LandWarNet and will be linked to the GIG. LandWarNet is the Army counterpart to the Air Force C2 Constellation and the enterprise network of the Navy's ForceNet, and includes 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 (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.<sup>13</sup>

**Bandwidth Needs.** According to John Stenbit, former Assistant Secretary of Defense for Networks and Information Integration (ASD/NII), the primary problem that must be overcome to make information for Network Centric Warfare (NCW) easily accessible through the GIG is meeting the demand for bandwidth.<sup>14</sup> 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.<sup>15</sup> 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.<sup>16</sup>

## 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

---

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

<sup>14</sup> 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.

<sup>15</sup> 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/>].

<sup>16</sup> CBO, *Issues Associated with the Global Information Grid Bandwidth Expansion*, Feb. 28, 2005, p. 15.

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 will 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).<sup>17</sup> 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 delivery.<sup>18</sup> 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.<sup>19</sup> The Defense Department has merged its Business Systems Modernization (BSM) effort with its Global Information Grid architecture project to ensure that all network architecture efforts comply with GIG standards.<sup>20</sup>

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?

---

<sup>17</sup> 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.

<sup>18</sup> Rich Tuttle, "New Organization to Stress Importance of Network Programs," *Aerospace Daily*, Jan. 30, 2004.

<sup>19</sup> Rich Tuttle, op. cit.

<sup>20</sup> Jason Miller, "DOD Builds on GIG Blueprint," *Government Computer News*, vol. 23, no. 1, Jan. 12, 2004.