

Moving Power to the Edge

By John P. Stenbit, Assistant Secretary of Defense

Networks and Information Integration/DoD Chief Information Officer (ASD (NII)/DoD CIO)

Introduction

Secretary Rumsfeld came to the Department of Defense two and a half years ago with a vision for transforming DoD to meet the changing, asymmetrical threats of a new and different world. True transformation can only be achieved by transforming the way we communicate, by making the network work for us, and by taking full advantage of Information Age technologies to ensure that our warfighters have immediate and direct access to the information they need. We are making great strides toward that goal.

When I arrived at the Pentagon in August 2001, I talked about the need to move toward net-centric warfare and operations — to create a network that had plenty of bandwidth and that people could trust, to populate that network with new dynamic sources of information, to protect it, and to ensure our adversaries do not have similar advantages. This effort is a driving force in enabling DoD's transformation. Our successes in Afghanistan and Iraq point to the progress we have already made within a relatively short time, and give us reason to be very optimistic about where we are headed.

By exploiting technological advances that continue to shrink the costs of bandwidth, information processing, and information storage, we are moving from the "smart push, smart push" regime of the past to a new "smart pull" paradigm where our warfighters — wherever they may be in the world — will be able, to "pull" from DoD, other U.S. agencies, and allied powers the information they (the warfighters) determine they need to complete their mission. This will move power from the center (headquarters) to the edge (fighters), and it is a transformation we must accomplish if our forces are to be able to operate with the speed and flexibility necessary to overcome the threat posed by small, hidden, dispersed, and fast-moving terrorist groups.

Technology determines how we can communicate and operate. This is illustrated by the differences between the telephone service of the 1970s (i.e., before voice messaging and wireless telephones), direct broadcast television, and the Internet. In the 1970s, when I was doing my first stint at the Pentagon (1973-77), we were in an era when communications bandwidth, information processing and information storage were all expensive. Consequently, we relied upon a telephone system as our fundamental information system because at the time it was the best system for optimizing use of those expensive resources.

Consider the limitations DoD operated under when it had to rely on the telephone system as its fundamental information system. Someone in DoD with valuable information first had to be smart enough to recognize that the information was valuable, and second, had to be smart enough to know to whom the information should be communicated. (How else would he or she know what telephone number or numbers to dial?) In other words, in the 1970s, DoD had to rely upon a smart push, smart push information system that relied, in turn, on the judgment and knowledge

of the few to push information to the many, rather than on the exponentially better judgment and knowledge that can be achieved when the brains and experience of the many are harnessed together. That telephone-based information system imposed additional limitations on the Department. Specifically, even if someone with information was smart enough to recognize its value and know to whom it should be communicated, there was nothing he could do if the latter wasn't at his phone when he called. That is, the person called had to be at the right place at the right time — what I have termed being "synchronous in time and place."

The limitations imposed by this system sometimes had serious adverse consequences. For example, there were two separate incidents before my first stint at DoD involving impending danger to two of our ships — the *Liberty* and the *Pueblo*. Because of the limits of the communication systems then in use, we were unable to share information that might have saved those ships.

Fortunately, technology has brought us a long way in a very short time. Our communications and information system today is a smart push system that takes advantage of the same broadcasting technology that has created commercial direct broadcast television. That is, someone at DoD just needs to be smart enough to recognize the value of the information they have and the need to push it to others. Having made that determination, they need only put the information on a transmitter and broadcast it to everyone with access to the transmitter. They don't have to determine who needs the information. Moreover, since the information is broadcast — rather than sent down a particular wire circuit to a particular receiver as was the case with our 1970s telephone system — it is available to anyone with a broadcast receiver. Recipients no longer need to be synchronous in place.

The price of processing and storage has gone down so much that we now can afford to have many people listen to all of the broadcast channels, store what they receive, and then put the information together to meet their own specifications. That's why Operation Iraqi Freedom worked as well as it did. That's also why in our post-September 11 action in Afghanistan, for example, a guy on a horse with a wooden saddle could broadcast, "*I need a bomb over there*," and another guy in a B-2 who had flown all night from Missouri could drop a Joint Direct Attack Munition (JDAM) right on "there."

Certainly, the smart push broadcast system represents a big improvement over the old smart push telephone system. However, it still relies upon the few to decide for the many what information is valuable and needs to be pushed to the many. It is in conflict with two basic truths: (1) Information consumers are the best judge of the information they need and; (2) Many brains working together are exponentially smarter than a single brain working in isolation.

That is why we are moving aggressively to put in place the satel-

lite laser and fiber optic bandwidth as well as the information processing and storage capacity that will enable us to complete the quantum leap to a network-centric smart pull information system linking all DoD's personnel, systems, and assets (including, as appropriate, other U.S. agencies as well as agencies and forces of other nations) so they may communicate, think, and act together.

The Internet is the closest we have to a commonly recognized model for the network-centric system we are building. Those with information need not be smart enough to ascertain the information's value or to whom it might be valuable. They can just post the information on the network and leave it to everyone else who is browsing the net (information consumers) to pull that information from the net, use it, assess its value, and offer (post) additional information. Information can be quickly exchanged by a nearly limitless number of participants dispersed all across the globe but connected to the network, i.e., many brains can be "networked" together to greatly accelerate learning and problem-solving just as we link computers together to crunch enormous amounts of data. The network of lasers, fiber optic lines, and information processing and information storing computers will be at the center of this network-centric model.

DoD's National Imaging and Mapping Agency (NIMA) illustrates the huge potential value to DoD of building a robust network-centric information, communication and warfighting system. NIMA has a Web site where the user can specify a particular geographic site or area and download (pull) all the latest satellite photos. That's the good news. The bad news is that the downloading is slow because there is insufficient bandwidth. And, of course, that underscores how critical it is that we rapidly put in place the bandwidth that is essential if we are, in fact, to achieve a robust, network-centric system that will link all our brains and other resources together to multiply our capabilities and make those capabilities available to be pulled (used) by those "at the edge" — most particularly America's fighting men and women — wherever they may be in the world.

Marketplaces of Information

Net-Centric Warfare allows users the ability to create and share a high level of awareness and to leverage this shared awareness. But achieving shared awareness alone will not guarantee success. We need to think about information differently as we move from a set of monopoly suppliers of information to an information marketplace. In essence, we want to create an environment where these five critical architectural tenets prevail:

◆ *"Only handle information once."* Collecting information and entering data multiple times is costly and adversely affects efficiency in both combat and business operations. The concept of only handling information once requires that processes be reengineered, and that technology and processes are integrated to minimize the time and effort dedicated to data collection and entry.

◆ *"Post before processing"* means that access to data for disparate needs is not delayed by unnecessary processing. Everyone is a provider and consumer of information. A provider has the responsibility to post data before using or manipulating it; consumers will have the technical capability to securely access the data they are cleared to access when they want it and in the format

they need.

◆ *"Users will pull data"* as needed instead of having massive amounts of information pushed to them regularly — regardless of whether it is needed. TPPU (Task, Post in parallel, Process in parallel, Use in parallel) means that information moves us away from the stovepiped information that characterizes the old TPED (Task, Process, Exploit and Disseminate). A key tenet of net-centric warfare is that the consumers of information are smarter than their sources about what is needed operationally right now and that they should be able to pull those data when they need it. Smart pull promotes speed instead of drawn out analysis. Further, the network will provide the access to information at multiple security levels (MSL), avoiding the technical challenges and high cost of Multi-Level Security (MLS) systems, which required users to have a trusted operating system to process information at multiple levels simultaneously.

◆ *"Collaboration technologies"* will be employed to assist users in making sense of the data that is pulled. For example, subject matter experts from diverse units or organizations are frequently called upon to come together to make sense out of special situations. The ability to pull expertise from within a unit as well as from across the Department is a value-added feature of a net-centric environment.

◆ *"A reliable network is key."* Diverse information pathways must be in place to ensure reliability. Security must be designed into networks and systems. Information assurance and interoperability — critical elements of "net-readiness," — must be the rule rather than the exception.

Interoperability

The approach to interoperability needs to change. The pace of advancing technology requires us to move from an approach that is based upon application standards to one based on data standards. The key is to give data users an opportunity to use the applications that make sense to them while maintaining the ability to exchange data. We also need to give more support to peer-to-peer relationships and information exchanges that transcend individual systems and organizations. Net-Centric Warfare involves a historic shift from platforms to the network. In effect, the single greatest contributor to combat power is the network itself. However, moving power to the edge will multiply the power that can be generated from a given set of assets and available information.

DoD's Net-Centric Transformation

The Department has undertaken key initiatives that provide a solid foundation for DoD's net-centric transformation. Just recently, I signed a policy memorandum that will institute the next generation Internet protocol, IPv6, throughout the Department by 2008, and bring DoD closer to the goal of net-centric warfare and operations. IPv6 will facilitate integration of the Global Information Grid — sensors, weapons, platforms, information and people and ensure that our warfighters are secure and connected in a fast-moving battlespace.

[Communications or the Transformational Communications Architecture, consists of the Global Information Grid Bandwidth Expansion \(GIG-BE\), the Joint Tactical Radio System \(JTRS\) and the Advanced Wideband System and Transformational Communica-](#)

[tion Satellite Efforts](#). This defines the transport element of the GIG and will be composed of three fully integrated segments. The terrestrial segment will be based on fiber optics and includes the GIG-BE. The wireless or radio segment will be based on the software programmable JTRS and its wideband network waveform. The space-based segment will be based on the Transformational Communications Satellite capability using lasers in space.

[GIG-BE](#). Current telecommunications lines are not robust enough to handle the volume of information needed for optimum strategic decision-making. The GIG-BE is designed to be robust enough to address current bandwidth constraints. It will use advanced fiber optic backbone and switching technology to upgrade telecommunications lines at DoD critical installations, and provide networked services with unprecedented bandwidth to operating forces and operational support activities. The GIG-BE will provide approximately 1,000 times the current capacity to critical DoD sites worldwide. New security technologies are being developed to keep pace with expanding capacities and enhance performance.

[Installation Bandwidth Modernization](#). Service-specific efforts to upgrade base or installation level communications capabilities will guarantee successful connectivity and ensure maximum benefits are obtained from the GIG-BE initiative. DoD components are developing installation bandwidth expansion strategies that will provide a bridge from the installation or base level telecommunications infrastructure to the expanded GIG.

[Joint Tactical Radio System \(JTRS\)](#). The radio-based or wireless segment will migrate to the software radio-based JTRS technology. Software radios are essentially computers that can be programmed to imitate any other type of radio and thus, can be readily configured to operate in different networks based on different standards. JTRS will also serve as a gateway between users with different hardware radios — a capability that speeds the transition to universal interoperability.

[Transformational Communications Satellite \(TSAT\)](#). The space-based segment of the transformational communications architecture is critical because many users are deployed in areas where optical fiber is unavailable, and many of our information sources — particularly intelligence, surveillance and reconnaissance capabilities — are airborne, making them especially difficult to link into a wideband network. TSAT, in essence, will extend the network's full capabilities to mobile and tactical users and will incorporate Internet protocol and laser communications capabilities into the Department's satellite communications constellation.

[Net-Centric Enterprise Services \(NCES\)](#). NCES provides a common set of information capabilities for the Global Information Grid to access, collect, process, store, disseminate and manage information on demand to warfighters, policy makers, and support personnel. These capabilities will enable shorter decision cycles by providing near real-time connectivity and computing power for warfighters and other users to get the right information at the right time and in the right format to meet operational, tactical, and mission support needs.

[Horizontal Fusion](#). Networks are essential to a net-centric environment, but they have limited value without quality data that are reliable, accessible, and usable in an integrated manner. The Horizontal Fusion Initiative will provide the tools and means to

integrate the smart pull of data with expert interpretations of the information. It will also provide tools to allow users to identify what data is available, access it, smartly pull and fuse it, and make sense of the data gathered. These tools require investing in data content and management, and the acquisition of commercial applications. While the initial focus is on intelligence RDT&E (research, development, test and evaluation), lessons-learned from the intelligence community will be exported and employed by the DoD business communities of finance, logistics and personnel.

[Data/Information Management](#). Computers and communications networks process, transport and deliver data. Horizontal fusion tools provide the means to search for, pull and fuse data from a myriad of sources, and allow users to make sense of data. Clearly, the crux of it all is "the data" — its visibility, accessibility, trustworthiness and understandability. Accordingly, the DoD Data Management Strategy has evolved with several features. For example, it emphasizes the use of catalogs, registries and other "search" services so that users can discover the existence of data with or without prior knowledge of its existence. It addresses means by which data is posted, tagged, advertised, retrieved and governed, as well as methods that facilitate trust in the data.

[Joint Strike Fighter \(JSF\)](#). Although the F-35's super cruiser capability, reduced radar signature, and vertical take off and landing capability are impressive, it is the aircraft's advanced avionics, sensor/radar and communications systems that truly stand out. They are designed to facilitate interoperability — enabling the JSF to exchange information with over 100 U.S. and allied platforms or systems including AWACS, JSTARS, sensors, aircraft, UAV ground stations, etc., — and also to be usable with new technology as it becomes available. Consequently, these avionics, sensor/radar and communications systems make the JSF particularly well suited for net-centric warfare where unhindered communication is an essential element, while helping to ensure that JSF will not be rendered obsolete anytime soon by the rapid evolution of technology. JSF, in essence, will plug into the net to satisfy its needs for information while also providing information to other platforms on the net.

[Business Modernization](#). The business community supports the warfighter and must be incorporated in business functions. The Under Secretary of Defense (Comptroller)/Chief Financial Officer is leading an effort to transform business processes. The CIO community's involvement includes assessment of architecture products for compliance with the Global Information Grid architecture; promoting business process improvements and ensuring that net-centric architectural tenets are reflected in these improvements; system acquisition oversight; and providing for the IT infrastructure and ensuring that its capabilities are in sync with the business functions' requirements for these capabilities.

[Information Assurance](#). The vision, *"People throughout the trusted, dependable and ubiquitous network are empowered by their ability to access information and recognized for the inputs they provide,"* holds profound implications for the Department's information assurance program. Because trust and confidence in our information is a primary concern when developing and deploying the information network and providing needed services, none of our critical systems, networks, platforms, and sensors can be deployed without the necessary security and interoperability capabilities

to make them net-ready. As such, our information assurance program has developed a strategy that supports this concept and has focused on providing the Department with robust protections, agile network defenses, integrated situational awareness, transformational assurance capabilities, and a professional, highly aware and trained workforce. Each of these elements works together to provide the necessary dynamic and agile information assurance capabilities for a net-centric force. I view these capabilities as integral to our efforts to transform the communications capabilities of the Department and see information assurance as critical to successful business and warfighter operations.

We are working hard to put all these pieces in place, and to institute a seamless, common network linking the Department and the Services. This new, integrated network will discourage anti-collaborative behaviors and allow us to exploit Information Age technology to our fullest advantage and turn the network into the single greatest contributor to combat power.



Mr. Stenbit became Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (C3I) on August 7, 2001, and now serves as Assistant Secretary of Defense of the C3I successor organization, Networks and Information Integration/Department of Defense Chief Information Officer. His career spans over 30 years of public and private sector service in the telecommunications and the command and control fields.

His public service includes four years at the Department of Defense from 1973 to 1977, serving for two years as principal deputy director of telecommunications and command and control systems, and two years as staff specialist for Worldwide Command and Control Systems in the Office of the Secretary of Defense.

Mr. Stenbit previously was an executive vice president of TRW, retiring in May 2001. He joined TRW in 1968, and was responsible for the planning and analysis of advanced satellite surveillance systems. Prior to joining TRW, he held a position with the Aerospace Corporation involving command and control systems for missiles and satellites, and satellite data compression and pattern recognition. During this time, he was a Fulbright Fellow and Aerospace Corporation Fellow at the Technische Hogeschool, Eindhoven, Netherlands, concentrating on coding theory and data compression.

He has chaired the Science and Technology Advisory Panel to the Director of Central Intelligence, and served as member of the Science Advisory Group to the directors of Naval Intelligence and the Defense Communications Agency. He also chaired the Research, Engineering and Development Advisory Committee for the Administrator of the Federal Aviation Administration. He has served on the Defense Science Advisory Board, the Navy Studies Board, and the National Research Council Manufacturing Board.

In 1999, Mr. Stenbit was inducted into the National Academy of Engineering.

Mr. Stenbit holds bachelor's and master's degrees in electrical engineering from the California Institute of Technology. He is a member of Tau Beta Pi, the engineering honor society. □

“The Umbrella Program has been and continues to be a cornerstone of the ESI project ...”



Talking with Jim Clausen OASD (NII)/DoD CIO ESI Working Group Co-Chair

The Enterprise Software Initiative (ESI) is a joint project designed to implement a software enterprise management process within the Department of Defense (DoD). The main problem identified with procuring software for DoD is that the software (including price, acquisition cost, distribution, training, maintenance, and support) costs too much. ESI objectives are to save money and improve information sharing. By pooling commercial software requirements and presenting a single negotiating position to leading software vendors, ESI provides pricing advantages not otherwise available to individual Services and Agencies. ESI's initial focus is on DoD common-use, standards-compliant software COTS software products.

CHIPS: *How does ITEC-Direct and the DON IT Umbrella Program (www.it-umbrella.navy.mil) fit into the ESI program?*

Mr. Clausen: The Umbrella Program fulfills the Navy's duties as ESI Executive Agent for Office Automation Tools and Enterprise Resource Planning software. The Program Manager, Barbara Johnson and her whole team, Linda Greenwade, Peggy Harpe and the ITEC-Direct group have been very supportive and proactive in pushing the ESI project. The ITEC-Direct (www.itec-direct.navy.mil) Web site is great and the team is customer-focused. I am amazed at what they have accomplished and at what they continue to do.

CHIPS: *How do you gather requirements for the IT products and services offered to DoD customers?*

Mr. Clausen: We follow the money and leverage the marketplace. We continually monitor customer interest levels by collecting data to see who is purchasing, and what they are purchasing. As Service or Agency buyers purchase, or plan to acquire significant amounts of particular software products, we look into the feasibility of expanding the scope of their contracts for the benefit of all DoD buyers. Then we assign an Executive Agent, who develops an acquisition strategy and a business plan. We discuss this strategy and reach consensus within the group. The Executive Agent, through their Software Product Manager (SPM) then begins negotiations with the software publisher. What usually results is a BPA off the GSA Schedule; with substantial pricing discounts. For example, as he observed that there was substantial interest in the Navy for Merant software, Floyd Groce (Department of the Navy representative and co-chair of the ESI Working Group) brought the information to one of the bi-weekly ESI Working Group meetings. The group eventually approved the Navy's plan to move forward with an agreement, which included some up-front funding, resulting in a pre-purchased inventory for Navy customers, and a BPA for DoD-wide use priced at 21 percent off GSA Federal Supply Service (FSS).