

INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Information Superiority for the Warfighter
John J. Garstka

Guest Presentations, Spring 2000

Charles E. Allen, Albert J. Edmonds, John J. Garstka,
Timothy G. Hoechst, Hans Mark, Dale W. Meyerrose,
Mark C. Montgomery, Scott A. Snook

October 2001

Program on Information Resources Policy



Center for Information Policy Research



Harvard University

The Program on Information Resources Policy is jointly sponsored by
Harvard University and the Center for Information Policy Research.

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

Copyright © 2001 by the President and Fellows of Harvard College. Not to be
reproduced in any form without written consent from the Program on
Information Resources Policy, Harvard University, Maxwell Dworkin 125,
33 Oxford Street, Cambridge MA 02138. (617) 495-4114

E-mail: pirp@deas.harvard.edu URL: <http://www.pirp.harvard.edu>
ISBN 1-879716-74-7 **I-01-1**

October 2001

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University

Center for Information Policy Research

Affiliates

Anonymous Startup
AT&T Corp.
Australian Telecommunications Users Group
BellSouth Corp.
The Boeing Company
Booz•Allen & Hamilton, Inc.
Center for Excellence in Education
CIRCIT at RMIT (Australia)
Commission of the European Communities
Critical Path
CyraCom International
DACOM (Korea)
ETRI (Korea)
Fujitsu Research Institute (Japan)
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
Hitachi Research Institute (Japan)
IBM Corp.
Korea Telecom
Lee Enterprises, Inc.
Lexis–Nexis
John and Mary R. Markle Foundation
Microsoft Corp.
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
NEC Corp. (Japan)
NEST–Boston

Nippon Telegraph & Telephone Corp
(Japan)
PDS Consulting
PetaData Holdings, Inc.
Research Institute of
Telecommunications
and Economics (Japan)
Samara Associates
Sonexis
Strategy Assistance Services
United States Government:
Department of Commerce
National Telecommunications and
Information Administration
Department of Defense
National Defense University
Department of Health and Human
Services
National Library of Medicine
Department of the Treasury
Office of the Comptroller of the
Currency
Federal Communications Commission
National Security Agency
United States Postal Service
Upoc
Verizon

Information Superiority for the Warfighter

John J. Garstka

April 20, 2000

John J. Garstka is the chief technology officer for the Directorate for C4 [Command, Control, Communications, and Computer] Systems, Joint Staff [JCS/J-6]. In this capacity he is responsible for a broad range of issues associated with information superiority and network-centric warfare [NCW]. As a recognized thought leader in the area of NCW, he has published several books and articles, including "Network Centric Warfare—Its Origin and Future" (with Vice Admiral Arthur K. Cebrowski), Proceedings of the U.S. Naval Institute (January 1998); Network Centric Warfare: Developing and Leveraging Information Superiority (May 1999); "Network Centric Warfare: An Overview of Emerging Theory," PHALANX (December 2000); the Department of Defense [DOD] Report to Congress on Network Centric Warfare (July 2001); and Understanding Information Age Warfare (September 2001).¹ He has presented over 300 briefings and seminars on information superiority and NCW to military and commercial audiences worldwide. Prior to joining the Joint Staff, Mr. Garstka was a senior systems engineer at Cambridge Research Associates, where he led consulting assignments for commercial and government customers. Previously, he served for ten years as an officer in the U.S. Air Force, with assignments on the Air Staff and at the U.S. Air Force Space and Missile Center. He is a distinguished graduate of the U.S. Air Force Academy, where he earned a B.S. in mathematics, and has earned an M.S. in engineering-economic systems at Stanford University, where he studied as a Hertz Fellow. Mr. Garstka is also an officer in the U.S. Air Force Reserve.

Oettinger: As I trust all of you know from the e-mail we sent you, the bad news is that General [John L.] Woodward has been preempted. The good news is that, in his place, we have the pleasure of welcoming John Garstka, who is an old friend. You've read his biography and so normally I wouldn't say much more about it, but the circumstances are rather special. He got an ear infection yesterday, and instead of flying up here he rode the train. This is heroism above and beyond the call of duty, and I just want you all to be aware of this special effort. Not only that, but he's been short on sleep. He is the long-time father of three boys and the very recent father of a

¹David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington, D.C.: Command and Control Research Program [CCRP] Press, May 1999); *Network Centric Warfare: Department of Defense Report to Congress* (Washington, D.C.: U.S. Department of Defense, July 2000); and David S. Alberts, John J. Garstka, Richard E. Hayes, and David A. Signori, *Understanding Information Age Warfare* (Washington, D.C.: CCRP Press, September 2001), [On-line]. URL: http://www.dodccrp.org/NCW/NCW_report/start.htm

baby girl, and so he has committed another act of heroism by tearing himself away from that new addition to come and be with us. It's customary for the father to give others cigars, but we figured that given the occasion we'd give him a cigar instead.

Garstka: Thank you very much, Tony.

Oettinger: Congratulations and best wishes! So saying, I turn it over to John Garstka.

Student: I'll bet his wife will make him go outside to smoke it!

Student: He's not around the baby now.

Garstka: First, I want to pass on General Woodward's regrets. As some of you may be aware, he is in the process of going back to the Air Staff to be the Air Force SC [senior communicator], in charge of communications and computers, and some transition responsibilities have come up. I spoke with him yesterday afternoon, and he just wanted to make sure that I communicated how sorry he is not to be here with you.

The presentation that I'm going to share with you this afternoon is about 80 percent what he would have shown you and about 20 percent my own insights to amplify his points. Because this presentation is for you, if at any point you have questions, please don't hesitate to ask. My objective here is to walk away having answered most of your questions or at least given you a Web site to look at if some of your questions weren't answered.

Today I'm going to talk about information superiority as it's defined in *Joint Vision 2010*,² and then I'm going to share with you some insights that have evolved recently. I'm going to spend a good bit of time talking about the power of networking and the relationship between the power of the network and network-centric operations. Then I'm going to talk about General Woodward's vision of the Global Information Grid [GIG], which the chairman [of the Joint Chiefs of Staff] supports in his posture statement. I'll mention some of the things we're doing to implement the grid and then wrap it up with questions and answers.

I'm sure many of you had the chance to read *Joint Vision 2010*. It came out in 1996, and it was important, for at least two reasons. First of all, it represented the first *joint* vision. The services have always had vision documents, but this was the first time the chairman of the JCS had said, "We're going to have a vision for the future of joint warfare." The second point that's worthy of note is that this document formalized information superiority as a warfighting concept. It didn't just say, "Information superiority is one of these nice-to-have things, sort of like a communicator employment act." Instead, it said that the concept of information superiority is central to warfare in the future, and that figuring out how to establish and maintain it is key to enabling the emerging operational concepts that were referred to as dominant maneuver, precision engagement, focused logistics, and full-dimensional protection. The objective was to figure out what this means, not only at the high end of operations but also across the spectrum of conflict. Consequently, we use the term "full spectrum dominance."

This is the definition of information superiority in *Joint Vision 2010* (**Figure 1**). It's difficult to figure out exactly how collecting, processing, and disseminating an uninterrupted flow of

²Chairman of the Joint Chiefs of Staff, *Joint Vision 2010* (Washington, D.C.: Office of the Chairman of the Joint Chiefs of Staff, 1996), [On-line]. URL: <http://www.dtic.mil/jv2010/jvpub.htm>

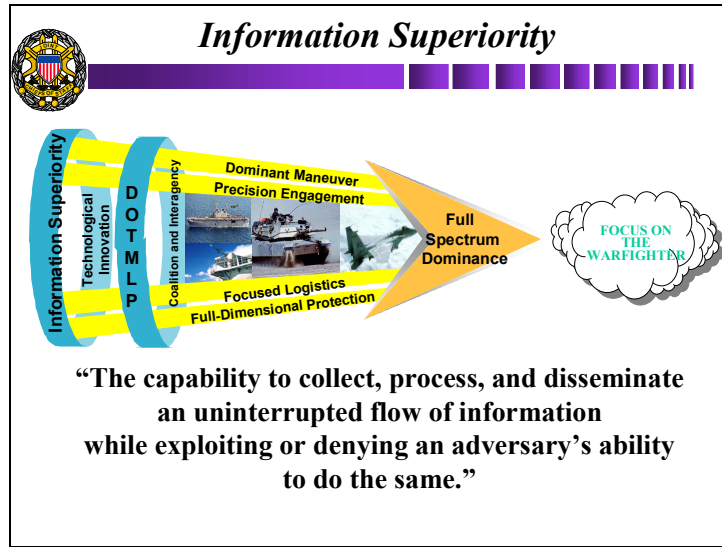
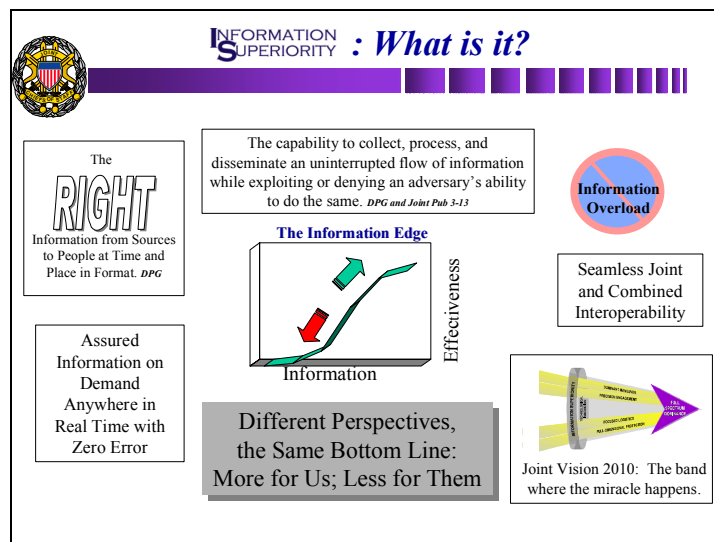


Figure 1

information while exploiting or denying an adversary’s ability to do the same thing is going to enable us to achieve full spectrum dominance. Trying to undo that Gordian knot has been one of my areas of focus and concentration for the last couple of years. The concept of network-centric warfare really emerged out of an effort to address those issues. You’ll see some of the insights that we’ve developed in the slides that follow.

Some of us who have been thinking about this have realized that when people use the term “information superiority” they use it to mean a lot of different things. Some of those things are highlighted on this slide (Figure 2). Recently, when we were doing some research, we came

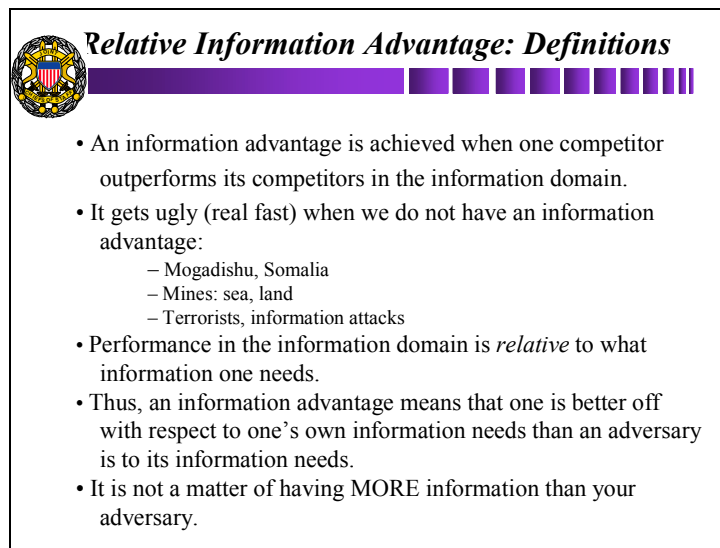


DPG = Defense Planning Guidance

Figure 2

up with an analogy that we think is at least useful to a first order of magnitude. It's an analogy between the way we use the term information superiority today and the way we need to use it in the future. We think there's an analogy between the way we need to use it in the future and the way the Eskimos describe snow. The Eskimos have fifteen unique terms for snow. There's fresh snow; there's snow that you can make an igloo out of; there's snow that's been on the ground for a couple of months; there's snow that's associated with a blizzard; and so on. The reason they have these terms and make these distinctions is that it's important to them. These words didn't just spring up instantaneously. They are part of their culture, part of the way their mental models are shaped.

Consequently, we've realized that we really need to work on our vocabulary. We need to be able to make some subtle distinctions. We're not at the point yet where we've figured out how to do that. We just recognize that there's a need to be more precise about what we mean by information superiority, relative information advantage, et cetera (**Figure 3**). One of the things that has become abundantly clear is that information superiority isn't absolute. Information superiority is relevant in a competitive domain, because warfare is a competitive domain and the concept of information superiority has to be measured relative to each adversary's needs. It also becomes clear that when we don't have information superiority, or when we don't have a relative information advantage, things get ugly fast. Some examples are highlighted on the slide.



Relative Information Advantage: Definitions

- An information advantage is achieved when one competitor outperforms its competitors in the information domain.
- It gets ugly (real fast) when we do not have an information advantage:
 - Mogadishu, Somalia
 - Mines: sea, land
 - Terrorists, information attacks
- Performance in the information domain is *relative* to what information one needs.
- Thus, an information advantage means that one is better off with respect to one's own information needs than an adversary is to its information needs.
- It is not a matter of having MORE information than your adversary.

Figure 3

It's interesting to point out that in many cases when people talk about asymmetric warfare bundled in that is information asymmetry. Because of the nature of that asymmetric type of conflict, there's an embedded information asymmetry that's more or less implicit. It isn't explicit. Some of the ongoing discussion that I'm part of in the Department of Defense [DOD] is about making those relationships explicit.

This slide (**Figure 4**) came out of a RAND document on rapidly deployable ground forces for the future. It introduces the concept of our taking a first-order perspective on the concept of relative information advantage. Let me explain some of the attributes on this slide. The vertical

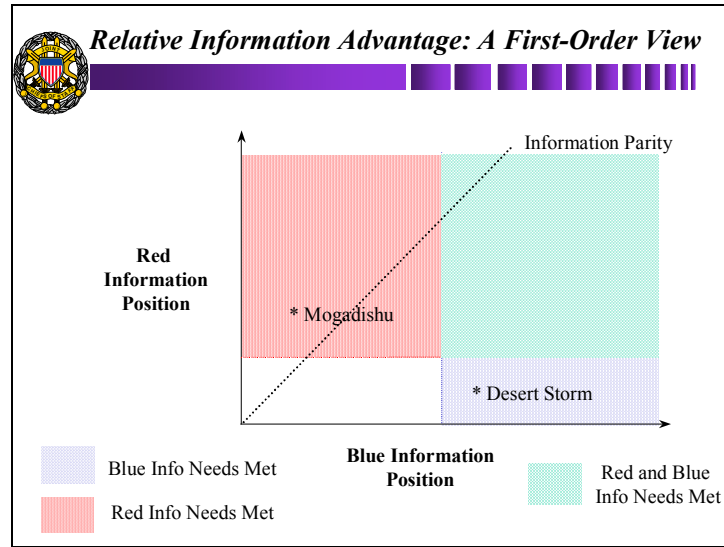


Figure 4

axis corresponds to the red information position and the horizontal axis to the blue information position. In the red-stippled area, red's needs are met, and in the blue-stippled area, blue's needs are met. Don't get too wrapped up in the relative position of the lines. We haven't quite figured out how to make this precise in quantitative terms.

Student: Just so the class understands the jargon, red is the enemy, blue is friendly.

Garstka: Thank you for that clarification. For instance, some of you may have had the chance to read *Black Hawk Down*, a very exciting book about some things that went wrong.³ It's clear from reading the book that the adversary in that situation [the Army Ranger operations in Somalia during Operation Restore Hope, 1991] had an information advantage relative to their needs, and in some cases we forfeited a potential information advantage. It wasn't intentional; it was just that in the fog and friction of warfare our guys thought it was going to be a short operation, and they left their night-vision goggles behind. Then, when things went wrong, one of the things that would have given them an information advantage had been left on the table. The information component comes through clearly in that book. You don't have to spend too much time going over the facts and the evidence from *Black Hawk Down* to realize that lack of an information advantage is probably what happened there.

If you think about the situation prior to the allied invasion of Normandy, you can see that the allied commanders tried to create this type of situation: a relative information advantage. They did that, for instance, by flying two sorties over Calais for every single sortie that was flown over the Normandy beaches. The whole concept of putting together a dummy set of forces and having Patton seen in the area across the Channel from Calais was all about trying to create that relative information advantage.

Of course, this slide shows a one-dimensional simplification of the problem. It's clear that there are lots of different dimensions to the information domain, and we try to highlight that in the next slide (**Figure 5**). In the following slide (**Figure 6**), we get at some of the finer grained

³Mark Bowden, *Black Hawk Down: A Story of Modern War* (Thorndike, Me.: G.K. Hall, 2000).

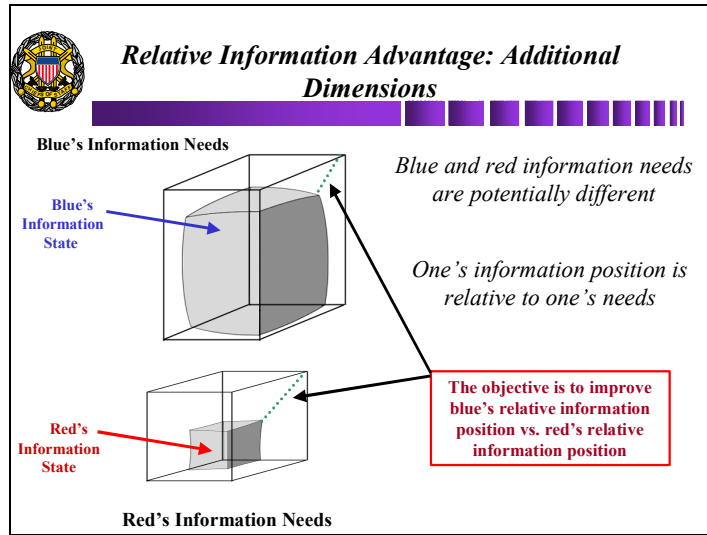
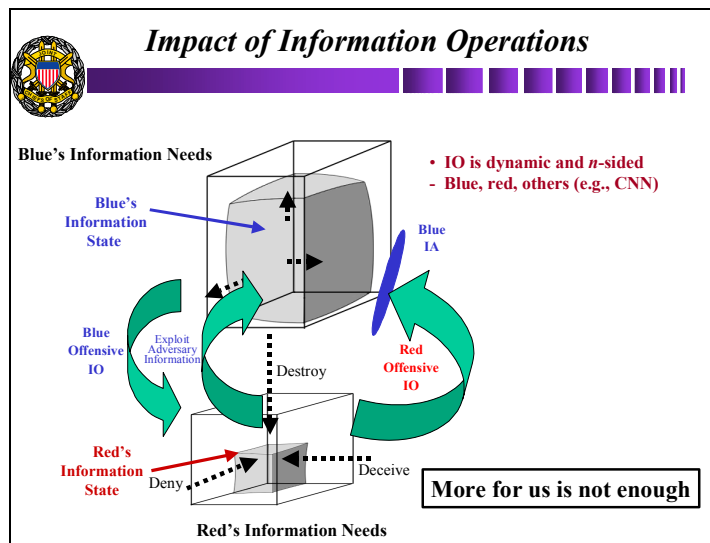


Figure 5



IO = information operations

Figure 6

details associated, for instance, with the fact that part of establishing information superiority and a relative information advantage has to do with what one force can do with respect to information operations, and that one of the challenges to each force is the ability to protect its information. Some of these subtle attributes are highlighted here.

It's also important to understand that there aren't just two players in this game. For instance, the worldwide press played a role in the situation in Mogadishu, as characterized in *Black Hawk Down*, and during Operation Allied Force [in Kosovo, 1999], so they're something of a wildcard in this information conflict.

Student: Could you explain the cube within the cube?

Garstka: The outer cube is supposed to represent blue's information needs. The inner surface represents the extent to which we have an information position. What we're trying at least to intimate in this diagram is that in this situation an adversary's information needs are less, but their position relative to their needs is lower than ours. Even though our information needs are greater in this situation, more of those needs are met. For instance, in our actual situation today, when we employ precision weapons that require mensurated GPS [Global Positioning System] coordinates, there's a degree of richness in the information domain that's required for taking something out with a 200-pound bomb that isn't there with a 2,000-pound bomb. For lots of different reasons, that's where we decided we want to operate. If an adversary wanted to operate with 2,000-pound bombs or with chemical or biological weapons, the degree of precision required for employing those weapons would not be nearly so high.

Oettinger: Let me make what may be a provocative statement, because I'd like to get your reaction to it, and you can either amplify on it now or come back to it later. It strikes me that there's a certain deceptive simplicity to this diagram [Fig. 6], even though it's a fairly complicated one. Deny, destroy, and deceive are all in the realm of information operations, but they're very different. What you describe with General Patton and Normandy versus Calais and so on is kind of in the psyops [psychological operations] and deception area, which seems to involve very different skills and outlooks and so on, at least traditionally, from lobbing a bomb on somebody's comm center. To put all of that under the rubric of information operations strikes me as overly simplistic.

Garstka: I'm not attempting to do that at all. During the discussion over lunch, we said that it's important to distinguish between the information domain and the cognitive domain. In many cases you influence the cognitive domain by what you put in the information domain. When our special forces dropped leaflets during Allied Force, that was in the information domain, but the leaflets represented paper with information on them that was targeted at the cognitive domain. It's important to understand that that we're using the term "information operations" today, but there's a cognitive domain focus and an information domain focus. You're seeing a work in progress here, as we've discussed previously.

It's clear when we look at ourselves as a joint force that the warfighting environment is becoming increasingly information intensive (**Figure 7**). The requirements are being driven by a higher mobility, a higher operations tempo, and the desire to create massed effects in comparison to massed forces. All are driving us to a warfighting environment that's very intense from an information perspective.

Oettinger: Before you take that slide away, let me just make another comment. The class will be reading Van Creveld's book shortly,⁴ and, of course, mass is one of those concepts that also is defined in Clausewitz, et cetera. It's very important to note what John is saying here about "massed effects, not massed forces," because one of the reasons why works by authors such as Sun Tzu and Clausewitz have stayed on the reading list for so many centuries is that they tend to be very Delphic. The notion of "massed" is always true, but massed what? The explicit recognition here that you're talking about massed effects and not massed forces is one of those

⁴Martin Van Creveld, *Command in War* (Cambridge, Mass.: Harvard University Press, 1986).

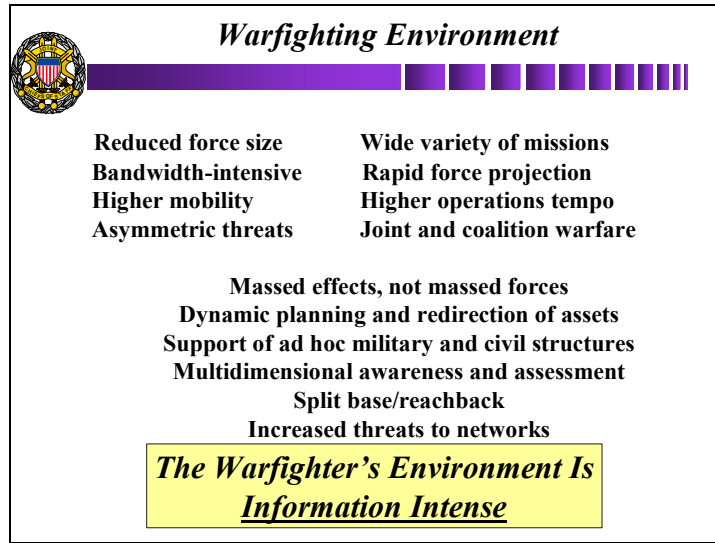


Figure 7

things that salvages the Delphic truth of the classic masters. It's like the Bible and everything else: it's all in the contemporary interpretation. This is a very important line that he sort of glossed over very quickly. It salvages these rather broad theories by reinterpreting the meaning of the central concepts. By reinterpreting "mass," you can say, "Oh yes, Clausewitz said it." He actually said something very Delphic. This is where the rubber meets the road.

Garstka: It's also important to note that when we look at each of the services' visions they're consistent with *Joint Vision 2010* (Figure 8): there's a recognition that information superiority must be a core competency of each service, and there's a recognition that the need to network the force is part of the entry fee, at least, at the vision level. It's also important to point out that we



Figure 8

have some help from a legislative perspective in the form of the Clinger–Cohen Act of 1996,⁵ which formalized the concept of the chief information officer [CIO]. Recently some directives have provided the CIO in the DOD with significant responsibilities and authorities.

Student: Before you go on, could you go over “DOTMLP” in the slide?

Garstka: That is shorthand for doctrine, organization, training, manpower, leadership, and personnel.

When we use the term “coevolution,” it’s basically saying that organization, training, processes, and materiel have to change together (**Figure 9**). You can’t change just one of them and expect anything significant to happen. One of the key insights that the C4 [command, control, communications, and computers] community has brought to the table is that part of the magic associated with 2010 is about combining the technology, the organization, and the doctrine and doing it in such a way that your processes can coevolve and your operational concepts can change to exploit the improvements in the information domain. One of the key entry fees is what General Woodward calls the Global Information Grid, which is sort of a network on steroids. It has a set of attributes that I will highlight later.

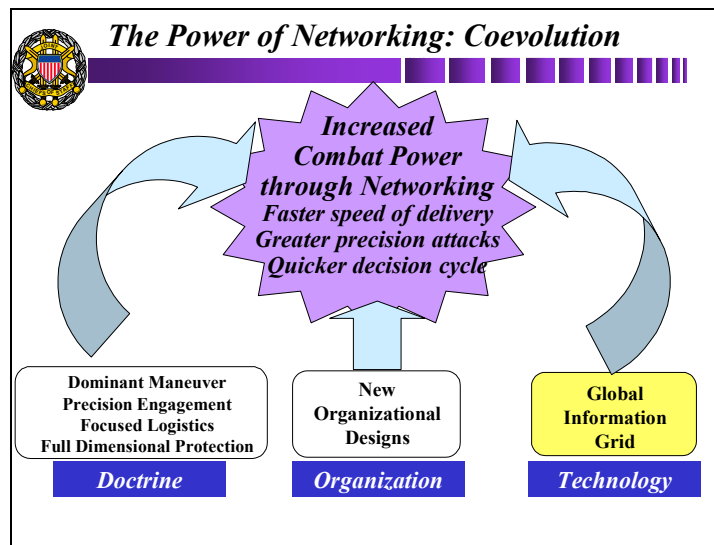


Figure 9

Oettinger: Some of the roots of this can be found in the seminar proceedings, specifically in the presentations by Admiral Jerry Tuttle.⁶

⁵The intent of the Clinger–Cohen Act of 1996, previously called the Information Technology Management Reform Act, is to improve government performance through the effective application of information technology.

⁶Jerry O. Tuttle, “Tailoring C³I Systems to Military Users,” in *Seminar on Command, Control, Communications, and Intelligence, Guest Presentations, Spring 1988* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-89-1, March 1989), and “The Copernican Pull,” in *Seminar on Intelligence, Command and Control, Guest Presentations, Spring 1992* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-94-4, August 1994), [On-line]. URL: <http://www.pirp.harvard.edu/pubs/html>

Garstka: We're clearly standing on the shoulders of giants in this area. Some people have provided key leadership in helping us get to where we are today.

Student: Was this built upon the Navy's intranet initiative, or are they totally parallel, separate entities?

Garstka: No. I would say that there's increasingly a realization that they all fit together.

Student: But the Navy did it first. You created your intranet concept and got it funded and then organized, and now you have the Global Information Grid. It sounds as though they're just building on that theme.

Garstka: There's a realization that networking the force and networking the supporting infrastructure are part of the solution space. We're using the term Global Information Grid in the same way that people use the term Internet, but it has some different attributes because some parts of the grid aren't like the Internet at all and some other parts are. You'll see that in several of the slides.

I'm going to talk about the concept of the network and value creation (**Figure 10**), because if you want to talk about the power of the network, you're talking about combat power. If you're going to talk about combat power, you've got to be able to measure it. If you want to be able to pay for the network, you've got to understand its source, because you've got to help the customer understand that there's some bang for the buck.

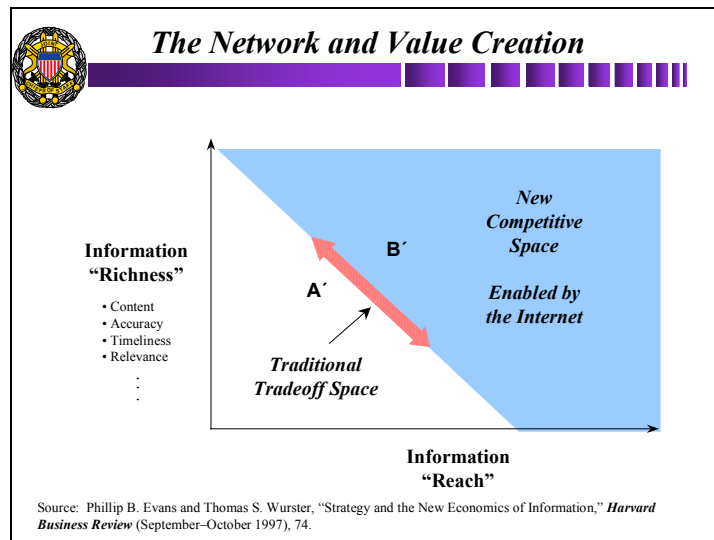


Figure 10

I'll spend just a couple of minutes going over some developments in the commercial sector that provide an intellectual point of departure. In 1997, two gentlemen who work at the Boston Consulting Group, Philip Evans and Thomas Wurster, wrote an article on "Strategy and the New Economics of Information" that showed up in the *Harvard Business Review*. Earlier this year,

they published a book called *Blown to Bits* that describes these concepts in more detail.⁷ Fundamentally, they assert that business and business strategy are about a tradeoff between information richness and information reach. When they use the term “richness,” they’re talking about the richness of information in terms of content, accuracy, timeliness, and relevance. They also talk about the richness of a relationship that a customer has with a client. Then they talk about the concept of reach. They assert that strategy has always been about where you want to operate in this kind of information isoquant, which is defined by the economics of information. They say that what the Internet has done is change the economics of information by several orders of magnitude.

To see the forest for the trees you sometimes have to operate at the right level of abstraction, and this slide (**Figure 11**) attempts to get at that. The phone network has been out there a long time. It works. It’s reasonably reliable. But what does it do? It’s available twenty-four hours a day, seven days a week. It’s primarily an audio experience. It’s full duplex.⁸ It provides very timely information transport. Its service reach is exceptional. However, it doesn’t have a visual component; unless you’re on a party line, the capability for multiactor interactions is minimal; and short of dealing with one of those annoying “For this option, press 1; for that option, press 2; for this option press 3” processes, there isn’t really a capability for search and navigation.

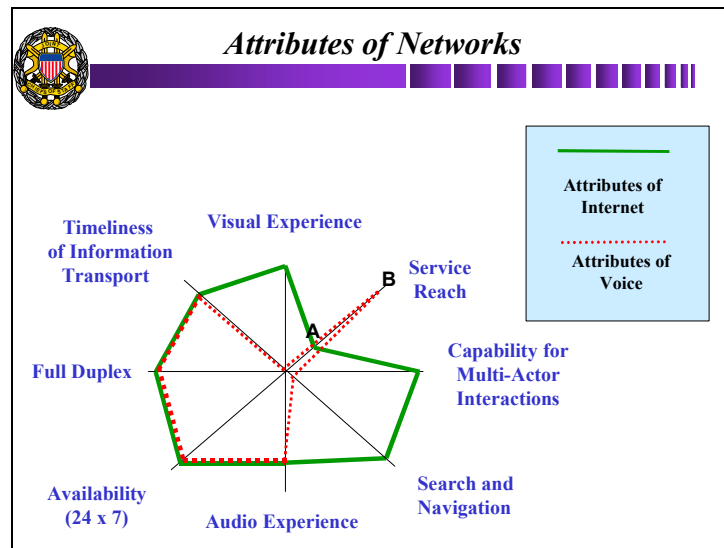


Figure 11

What has happened with the technologies of the Internet? If you’re using services such as AOL or Earthlink, like most of us, you’re using the phone line. What’s different? When you connect digital nodes, one of the things that you’re able to do is provide a visual experience. You’re able to offer the search and navigation functions that HTML [Hypertext Markup Language] and browsers have been able to provide, and you’ve got the capability for multiactor

⁷Philip B. Evans and Thomas S. Wurster, *Blown to Bits: How the New Economics of Information Transforms Strategy* (Boston, Mass.: Harvard Business School Press, 2000).

⁸Full duplex allows simultaneous telecommunications in opposite directions.

interaction. This is one of the things that you can do in eBay. Before the Internet, it wasn't cost effective to enable those kinds of business models. Of course, today the service reach isn't what it is with the phone line, and everybody's excited about moving point A out to point B because it represents lots and lots of dollars [Fig. 11]. The whole reason for introducing that graphic is to point out the subtle differences that correspond to increases in richness and reach.

Student: You mean the curve shifts out, so the tradeoff is more favorable?

Garstka: To use a term that Bill Gates has used on at least one occasion, this represents an isoquantal shift. In other words, as you move from A' to B' in Figure 10, there's a line that corresponds to the economics of information. What's happening is that it keeps shifting. It used to be that it wasn't cost effective to operate out here. Even if you had the money, you couldn't do the things that you can do with the Internet.

To move further with this example, let's use a bookselling analogy (**Figure 12**). For instance, Borders, which is a traditional brick-and-mortar type of operation, could be represented as the asterisk in the arrow, and Amazon.com could be represented by the asterisk farther up and to the right, in the shaded area.

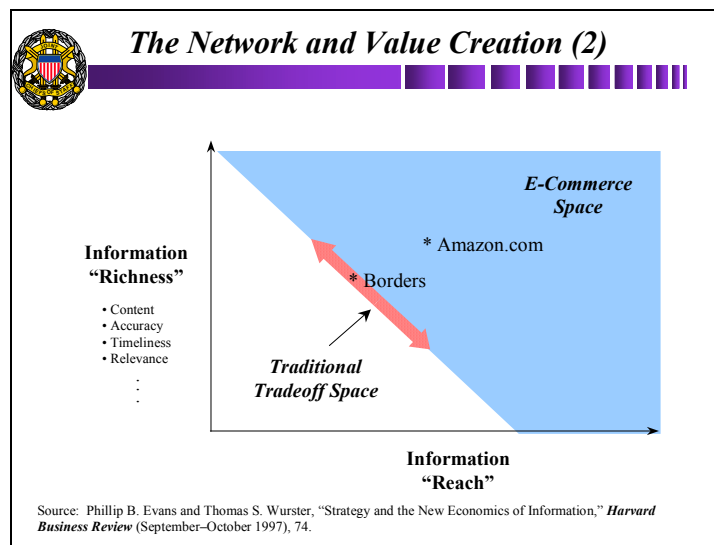


Figure 12

The following set of slides introduces a construct that we've developed for helping people to understand the relationship between reach, information richness, and value, because this is what it's all about (**Figure 13**). It doesn't make sense to operate out there if you can't provide value for a customer. It doesn't make sense to network the force if you can't generate combat power.

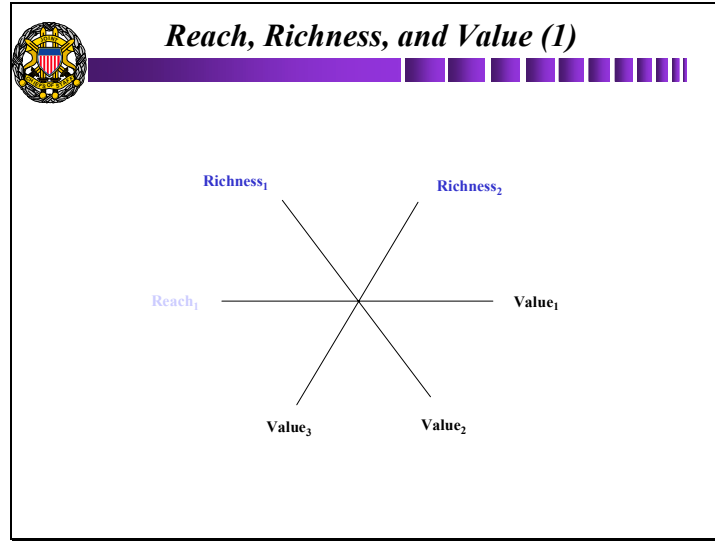


Figure 13

Consequently, if we continue with the bookselling analogy, we can see from this Kiviat diagram⁹ that there are certain attributes of brick and mortar that are very favorable (**Figure 14**). For instance, if you want to browse a book, it's very difficult to do on the Net. All you can get, for the most part, are the reviews. If you want to look at a book, read a couple of chapters, and decide if you want to spend money on that book, the best way to do it is at a bookstore. Similarly, if you find yourself in a situation that I have on several occasions, where it's nine o'clock in the

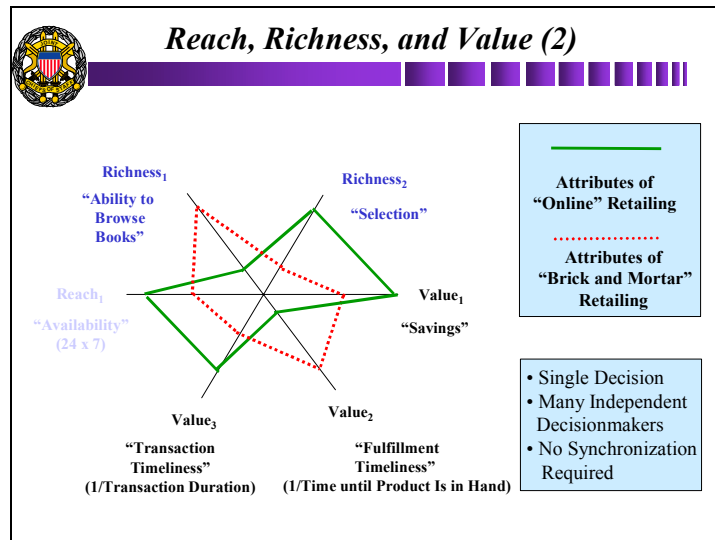


Figure 14

⁹A Kiviat diagram depicts various factors as the spokes of a wheel. The fractional value of each factor at a certain time, e.g., 75/100, determines a point on each spoke. Those points then determine the vertices of a polygon whose size and shape indicate the relative status of the various factors.

morning, your eight-year-old has a birthday party at two o'clock, and you need to find a book in the next five hours, you're not going to do it on-line because the fulfillment timelines won't support that. This is a very important attribute if you absolutely, positively need something in the next couple of hours.

However, if you're looking for selection, Amazon.com beats the traditional retailers hands down. The average number of books in a bookstore is about 250,000. Amazon has a couple of million. Similarly, there are some savings on most books. However, those of you who have tried to buy a traditional textbook on-line will have been rudely surprised to see that, when tax and shipping are factored in, the on-line purchase is more expensive in many cases. I went through the experience of buying a textbook for one of my previous professors at Stanford. The costs were the same for brick-and-mortar and on-line.

Let me give you an example where time was an issue. When I tried to track down the *Blown to Bits* book, I went into two Borders stores. One store said, "We have it in stock, but it's not on the shelf," so I spent forty minutes in that store. I went to another store and they couldn't find it either, even though they supposedly had it in stock. I spent two hours trying to find something because I wanted the book right then, and it turns out I would have spent less time doing it on-line. Similarly, if you are traveling overseas and you want to buy something after hours, the twenty-four-by-seven feature is relevant.

We can see, then, that how particular customers will respond to these attributes is a function of what's important to them. If you think about this for any length of time, you realize that a lot of these dot-com companies haven't quite figured out that the attributes they're providing aren't compelling enough, or haven't figured out how to make the economics of providing these attributes work.

Student: There's one other aspect to the relationship when you talk about fulfillment time. This is just an example. If I want to send somebody a present rather than hand it to the person, it's quicker on the Internet. Instead of going down to the store and buying it and wrapping it and then mailing it, I can just have it shipped directly.

Garstka: I've had that experience, and that's a good point. It makes sense to introduce that.

Oettinger: Can I throw in a small monkey wrench? I cannot resist. I had a recent experience, because I was a recipient of a gift. It was grapefruit sent from Florida, only it arrived with the return address of someone whom we didn't know.

Garstka: Were they good?

Oettinger: We didn't open it. We called in the bomb squad, because we've been close to being Unabomber victims, et cetera, and weren't going to open that package. When the bomb squad came around and we got the package open it was grapefruit, and it turned out to be from a neighbor who was visiting in Florida. The inside card gave a name we recognized. We could hear the guy saying on his squawk box, "Okay, they recognized this one," and everything calmed down. When our neighbor came back from Florida, we asked how this happened, and she said they must have screwed up. The guy on the return address was her brother. She had sent him to do the ordering and, in the process, the names got mixed up. It's an anomaly, but sending a gift

under circumstances where suspicious packages are not desirable leads to a strange, one-in-umpteenth-thousand side effect.

Garstka: Those things can happen.

Student: When you figure out the attributes for these systems, do you ask the customers if they want something that's overall interoperable or do you say, "These are the attributes we want to have"? Maybe you're going to get to it later, but all I'm saying is that one part of the organization values savings, and another part of the organization values fulfillment time. You couldn't show it graphically, but each of those involves a lot of difference.

Garstka: Right. In other words, every customer has a different template. Different people value these attributes differently.

Student: In your position in J-6, are you going out to the customers and trying to find the common points where their expectations or their attributes match?

Garstka: I would be leading you astray to let you think that we've thought about the Global Information Grid from this perspective. That's a place we want to go.

Oettinger: It's an extremely important point, and it presents itself somewhat differently depending on what we're talking about. It's well worth keeping in mind. On the intelligence side, let's say, where every customer is different, the adaptation of these nodes to the individual template can be a very serious problem. It would seem to me you'd go at it in a different way when this represents a procurement (which is your question), especially where the procurement may have to serve many people to be cost effective and where it may have to last for quite a while if it's a large capital investment. The charm of what is going on here is that you're providing a way of articulating these issues that I haven't seen before. While facing up to it in an explicit way doesn't necessarily produce a solution, it has the merit that at least you can talk about it.

Student: I spend a great deal of my time on Pacific Command staff answering this question from the JCS: "We're buying a new unmanned aerial vehicle system. Look at your war plans and tell us about your requirements." We're down there with the Pacific fleet and Pacific air forces. We've put in an enormous amount of time into doing what you're saying.

Garstka: With this diagram [Fig. 14] we're trying to develop a construct for relating information to value, because that's what the network does. Without the network, you couldn't do these things.

Student: It seems to me that there's another set of parameters that you haven't discussed, which is accuracy—the degree to which the information could be wrong, in the sense that there are legions of people who are building stuff deliberately designed to confuse us and to send wrong signals, imperfect information, or commercially traded decoys to us. For example, you've discussed positive attributes of information in this chart, and there ought to be some negative aspects. It's not quite so simple or so clear, because errors can be made in all kinds of funny directions. There ought to be a set of information qualities and information shortcomings. In some cases, shortcomings are not terribly important; in other cases, they are very important. To hit the wrong target would be most embarrassing.

Garstka: You'll see that in some of the slides that I'll bring up after we finish with this part of the presentation. It's also important to point out that in this particular situation every instantiation of value creation is a single decision. If you or Tony or I order a book, these are independent decisions. There's no self-synchronization or coordination involved. Value is created for each of us individually.

The reason why I spent the time going through these last couple of slides is that I want to develop an intellectual construct that helps us understand the relationship between information and combat power on the battlefield. We see a similar type of diagram here (**Figure 15**). We've got the information-reach attributes associated with interoperability and information attributes of shared awareness as related to richness, and we see that the ability to develop a relative information advantage with respect to an adversary has to do with being able to move in the directions of the arrows in the figure. Then we recognize that, because warfare is all about people doing things, there are important process measures that have to do with collaboration and synchronization. There are also some value attributes that the customer set—in this case the warfighter—cares about, and these can be represented by survivability, lethality, and operational tempo (**Figure 16**).

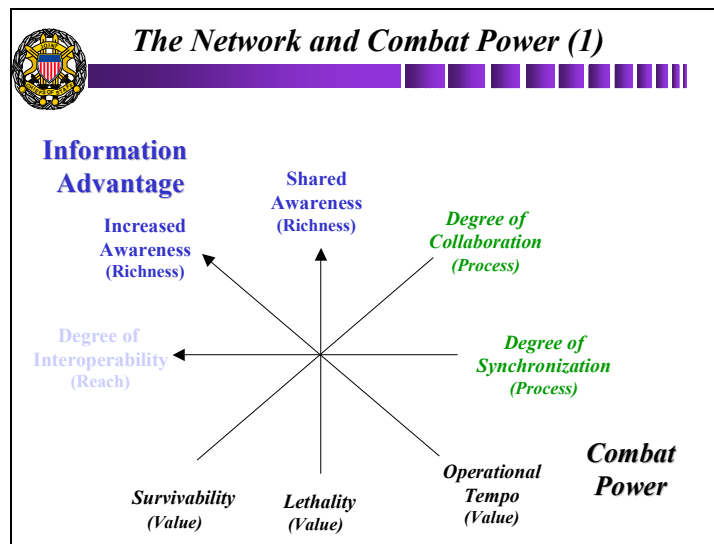


Figure 15

Student: On that slide, is your reach only the degree of interoperability?

Garstka: No. We're going to amplify that.

Student: So the unit includes sensors, for example, and how good your sensors are?

Garstka: Right. I'll cover that on some slides that follow. This is a first-order representation, and the objective is to introduce the template.

This (**Figure 17**) is, of course, a qualitative representation of the way things are today in some key mission areas with a platform-centric force. When you introduce the network, you get a significant capability to develop a relative information advantage. For instance, if an adversary

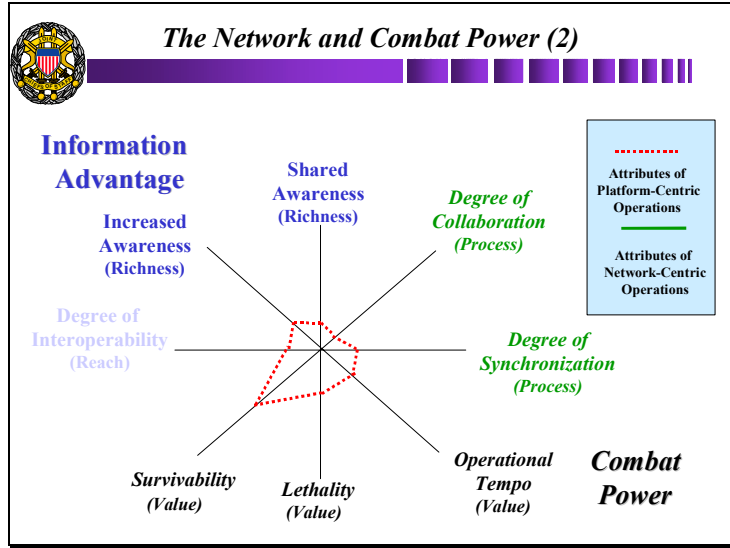


Figure 16

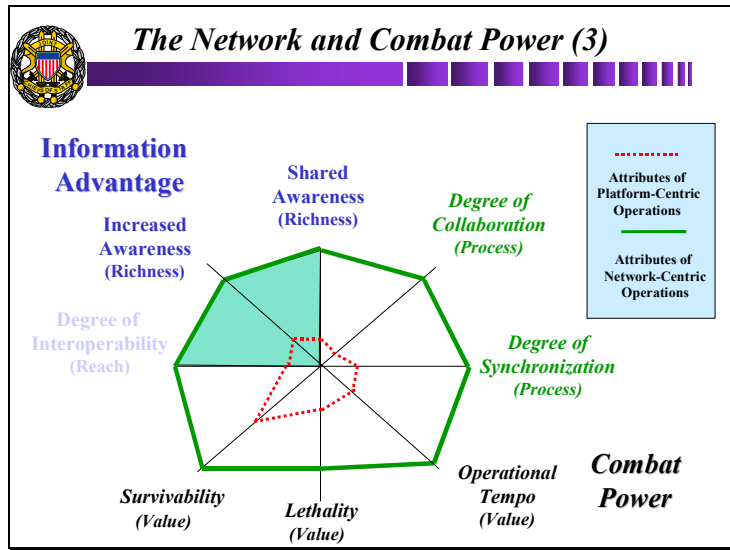


Figure 17

were operating in platform-centric mode and we were operating with network-centric operations, there's an inherent information advantage the warfighter can leverage by behavioral changes that result in information advantages. Some more detailed examples are covered in the *Network Centric Warfare* books.¹⁰

When one of our senior warfighters, Chief of Naval Operations Admiral Jay L. Johnson, talks about the shift from platform-centric to network-centric warfare, he is talking about new

¹⁰See note 1. The Department of Defense submitted its *Report to Congress on Network Centric Warfare* on July 27, 2001.

types of attributes (**Figure 18**). He's talking about being able to move away from a force that can be represented like the graphic in the upper left, where there are significant interoperability problems in both the voice and digital domains, toward a network-centric force where you've solved many of those interoperability problems. Again, the desired end-state is in the effects domain. You're not just doing this because you say that you could do it, or because you want to employ signal officers. You're doing this because you want to be able to generate effects on the battlefield that you couldn't get previously.

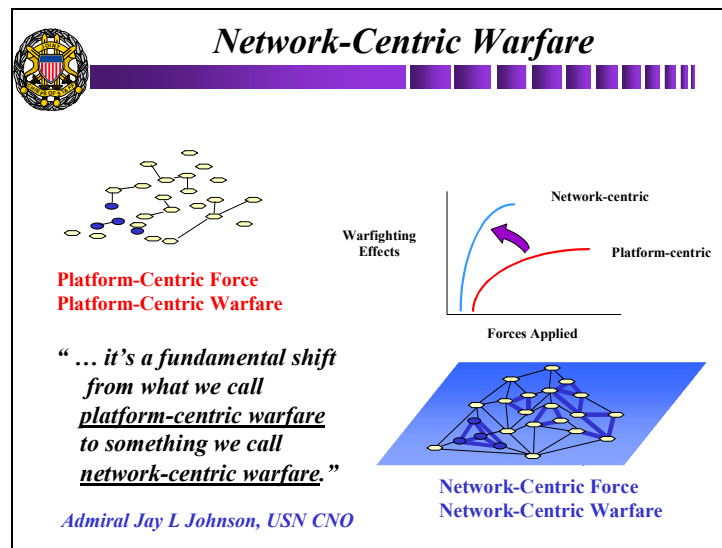


Figure 18

When somebody asks me, “John, what does the network-centric force look like?” I would first say that a network-centric force is an interoperable force. It provides commanders with the capability to network (or connect) sensors regardless of platform, decisionmakers regardless of location, or shooters regardless of service, and to do it dynamically. We haven't come across a warfighting force anywhere that can do that. Because of the legacy issues, et cetera, this doesn't exist. This is a desired end-state, and the GIG is key to helping us get there.

Oettinger: Again, my guess is that what he's describing here is going to take the rest of your careers to get anywhere near that desired end-state. It would be of interest and of some value to understand why things are moving faster in some areas than in others. I pointed out that you could find some stuff about the Navy in the particulars of those admirals for whom this is important and who talked here at the seminar.¹¹ Why the Navy? Because everything that he's describing here was harder for the Navy to do than for anybody else. The seminar has been going on now for twenty or more years. If you go back just a decade to around the time of the Gulf War, members of this seminar with a naval background—both students and presenters—would have regarded

¹¹See the following in various volumes of the *Seminar on Intelligence, Command, and Control* (Cambridge, Mass.: Harvard University Program on Information Resources Policy): Richard C. Macke, “C4I for the Warrior,” in *Guest Presentations, Spring 1992* (I-94-4, August 1994); Edward D. Sheaffer, “Naval Intelligence in the Post-Cold War Era,” in *Guest Presentations, Spring 1993* (I-94-5, August 1994); and the two presentations by Jerry O. Tuttle (see note 6), [On-line]. URL: <http://www.pirp.harvard.edu/pubs/html>

this as total science fiction. The complaint of one guy who was sitting at this table was that when he was at dock somewhere in Kuwait he had all kinds of connectivity, and then 100 yards off dock he was back in a world that a navigator at the time of the Romans or Greeks would have recognized: namely, he had hardly any communications at all. For the Navy, this gain is absolutely dramatic, and they've been riding it ever since. Where the Air Force and the Army are stuck with some legacy ideas and so on, the Navy had almost no legacy.

Garstka: Another point that came up over lunch was that the degree to which the services have made significant progress with respect to networking their forces is directly proportional to their desire to deal with casualties, in a certain sense. In other words, the Navy is very reluctant to lose a big capital ship. If you look at the areas in which the Navy introduced data links—first to help with the outer air battle, then with the cooperative engagement capability—they were all about that the Navy absolutely, positively wanted to make sure that they had a place to take off and land. In the Air Force, if you crater a runway, you fix it, but if you crater a carrier, it's at the bottom of the pond. There's a degree of focus on developing a competency for dealing with a threat and on using the network to solve that problem. You just didn't have that degree of focus in any of the other services.

I'd also say that one of the advantages that the Navy at least has had with respect to networking their surface combatants is that they were the first to be able to exploit Moore's law:¹² big ships, big computers. It's taken a while for the Army to be able to say, "I can put the performance I want on a tank at a price that makes sense." There are multiple factors involved.

When we talk about networking the force, what we're talking about is providing not only reach, which is what comes to mind most of the time, but also richness. This is an important point, because how you network the force and the type of network that you use to connect the force is a function of the reach and richness that you want to be able to provide.

Someone asked earlier about attributes. These are eight examples of attributes of richness in the information domain (**Figure 19**). They're far from complete, but they're representative. Timeliness is important: it addresses *when*. Relevance: *why*. Identification: *who*. Classification: *what*. Precise position location: *where*. The extent to which each of these measures of richness is important is a function of the type of mission you're trying to prosecute and your willingness to deal with casualties, or your willingness to deal with Blue on Blue. Similarly, one can look at some attributes of information reach (**Figure 20**). Again, these are some of the issues that we traditionally mention. If you take both of these diagrams together, you've got at least sixteen attributes, and you're starting to get to the type of delineation that the Eskimos have for snow. You can start thinking about different positions in the information domain and quantifying and making subtle, fine-grained distinctions about capabilities for operating in the information domain with these types of attributes.

¹²The observation made in 1965 by Gordon Moore, co-founder of Intel, that the number of transistors per square inch on integrated circuits [ICs] had doubled every year since the IC was invented. Moore predicted that this trend would continue for the foreseeable future. In subsequent years, the pace slowed down a bit, but data density on ICs has doubled approximately every eighteen months, and this is the current definition of Moore's law, which Moore himself has blessed. (Quoted from the Webopedia [On-line]. URL: http://webopedia.internet.com/TERM/M/Moores_Law.html)

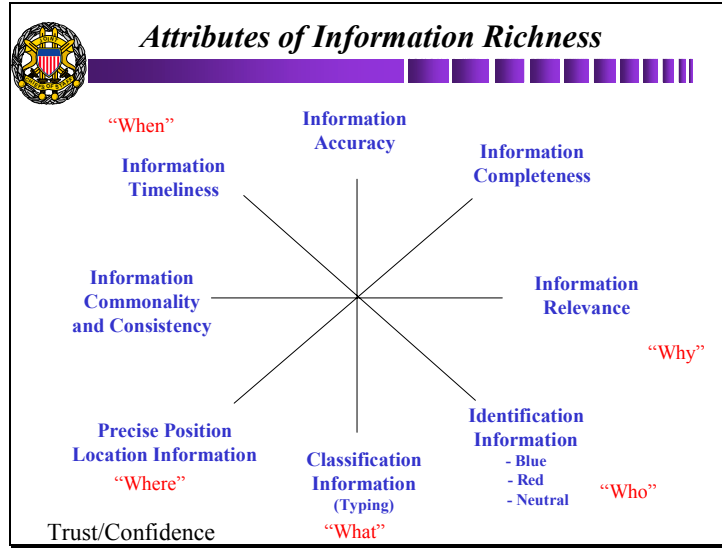


Figure 19

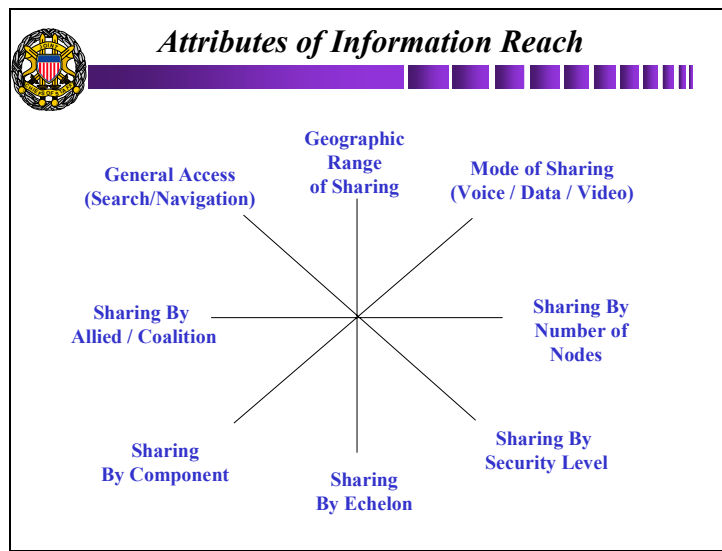


Figure 20

Oettinger: Forgive me for interrupting, but it's a measure of my interest. Each one of those is stressing the positive side and is a point on which decisionmakers will disagree. Each can therefore be a point of bureaucratic entrenchment over days, years, months, or decades. If you ask why, when all of this is so clear, it is going to take time to reach its end-state, one of the reasons (and again, I won't try to predict the importance of the mix) is that everyone involved will disagree on each of these.

Student: I'll go one step further. It won't be just bureaucratic disagreement. The different services, by nature of the different media they operate in, will have different environments.

Oettinger: That’s in your reading in Allard.¹³

Student: Is there an end-state, or is this a process that goes on indefinitely as long as warfare goes on?

Garstka: I think that it’s a continuous process, but what you’re looking at here is a potential way of describing capabilities of the grid. In other words, you can think about these as points along the way to the future. I’m not trying to intimate that we’re capable of doing this now on the Joint Staff. What we’re starting to realize is that one of the challenges we face when we talk about interoperability is that we don’t have these fine-grained distinctions. If we start operating in the attribute space, we can make some distinctions about, “Let’s agree that in the next two years we’re going to focus on *this* set of attributes, and, then, two years from now, on the other sets of attributes.” Right now, we don’t even have a fine-grained enough language to be able to disagree politely. That’s one of the challenges that we face.

Oettinger: I couldn’t agree more. Let me try to develop that point just a little bit further, because I think you’re stimulating an extraordinarily rich and invaluable discussion in this seminar. The very notion of an end-state, given the changes in the world, the changes in the technology, et cetera, is rapidly losing its usefulness. The dilemma is this: You talk about “process” and “ongoing,” and there isn’t a budget person or a procurement person in the world who understands that. The cultural gap between the kind of thinking that you’re hearing here today and the present reality in any organization that I’m aware of—military, civilian, U.S., or anywhere else on the globe—is enormous. The notion of thinking about this in terms of an ongoing process that may not have an end-state implies managers capable of managing a process that has no end-state. If you start thinking about that in terms of what it means when you have to make capital investments, it requires adjustments in thinking that none of us has made yet. There are highly revolutionary implications of what John is describing here—very blandly in some ways. It’s raising hell with all sorts of established thought, and so we’re very grateful to you (or, at least, I am) for your enabling us to share that.

Garstka: What’s interesting to reflect upon (the authors make this point in *Blown to Bits*) is that what the Internet has done is not just about connectivity; it’s also about standards for sharing information. The Internet has made it possible to solve these problems. It used to be that if a company that operated in the United States acquired a company based in another country, and that company was operating with a certain set of databases, there was an interoperability problem. The Internet has enabled companies in the commercial sector to solve interoperability problems that in the past were prohibitively expensive.

Oettinger: Up to a point, but the class has heard a briefing by Tim Hoechst, who is the technology guy at Oracle, pointing out that in his own company they can’t reach that ideal because of differing national legal structures that either require or prohibit the presence of certain

¹³C. Kenneth Allard, *Command, Control, and the Common Defense*, rev. ed. (Washington, D.C.: The Center for Advanced Concepts and Technology, National Defense University Press, 1996).

data elements.¹⁴ You have an overlay of the political on the technological, which makes this a very nasty, complicated managerial problem.

Student: In terms of the DOD, though, it's not going to be a political overlay, it's going to be a "human" overlay.

Garstka: It is both, because, for instance, when you talk about sharing by allied and coalition forces, it isn't just an issue of technology, it's an issue of whether we want to share this information. That's a political science issue.

Student: As we talk about this, it is a continuum, and the procuring and fielding of systems that can do these things will also be a continuum. It's going to be a phased type of thing. First, you've got to say, "Can we have this set of standards so we're all interoperable in all these attributes?" When we buy it, we must have in mind that it's positioning us to buy the next set of stuff, and that becomes incredibly complicated.

Garstka: As the discussion highlighted a couple of minutes ago, being able to introduce a construct like this enables people to say, "Let's focus on these couple of dimensions now, because they are the most important from a combat power perspective." We can't even have those discussions today, because we get this service bluster and it hides the fact that we don't have the skill set to have a dialogue.

Student: On this particular chart [Fig. 20], I, as a technical person, understand why you would want to share by security levels or why you would want to share by the number of nodes. But you mentioned earlier that you wanted to make decisions and so forth on the basis of some type of business value (combat value, in this particular case), and I'm wondering why these are not axes of business value? In other words, why "sharing by security level"? That's what a business manager is going to ask.

Garstka: I showed you a previous Kiviat diagram that had a subset of richness and reach dimensions and some value dimensions [Fig. 14]. This slide is just amplifying that one.

Student: I want reach for the same reason: because it adds business value.

Garstka: Right. I just can't figure out how to draw a diagram that's got fifty of these axes on it yet.

Student: I'm just talking about the terminology that you use to describe it. "Sharing by security level" means something to techies. If I'm a high-level manager, I have no idea what that buys me.

Garstka: What you need to be able to do is show the relationship between that concept and the business value of combat power.

Student: I'm just asking why the terminology that you use here is not based on business value.

Garstka: It's because I wanted to focus on these dimensions. On the earlier slides [Figs. 15, 16, and 17], survivability, lethality, and operational tempo are the business values. In Figure 17 I'm

¹⁴See Timothy G. Hoechst, "I3I: Information, Information, Information, and Information," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2000* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-01-1, July 2001), [On-line]. URL: <http://www.pirp.harvard.edu/pubs/html>

representing three out of potentially sixteen information attributes. I could just as easily have put sixteen different attribute lines in and then left the value attributes the same. For illustrative purposes, I broke them out, but this relationship between information and “value” is the construct that we’re working toward.

Student: What is the meaning of “end-state”: that you reach a point where you no longer have to change the way you analyze and look at things?

Garstka: Let me use an example. If you’re involved in a conflict and you want to terminate it there is a set of terms and conditions that represent a desired end-state. For instance, you want the adversary to pull back to a certain point. In some cases, people use those terms in business, in the sense that the desired end-state is a certain percentage of the marketshare. It’s just a term people use to describe a desired outcome.

Student: I still don’t understand why that is such a shift. I guess what we’re saying is that, traditionally, it’s been viewed as analyzing warfare to an end-state and now we’re looking at it in stages.

Garstka: No, the point that Dr. Oettinger was making is that, in the acquisition process, people traditionally thought of the acquisition of a product as being the end-state. It rolled out the door, you bought it, and you might do a couple of preplanned product improvements, but there was a definite end-state. In the information technology sector, the technologies are moving so fast that it doesn’t make sense to describe the GIG, for instance, in terms of an end-state. You might want to think about it in terms of different releases that are associated with a specific set of attributes, because that’s the way, for instance, that Microsoft rolls out products. You’re got Windows 95, you’ve got Windows 98, you’ve got Windows 2000, and it’s not clear what the end-state is. Each release reflects specific attributes associated with technological possibilities.

Student: When they fielded the first telephone system, they could not see what it would look like when everybody had a phone and a fax and everything. They just put it out there. They didn’t see the end-state. It wasn’t possible back then. We don’t know the end-state of the Internet.

Garstka: That’s right. What I want to do here, as I wrap up this section, is highlight in some cases subtle distinctions between richness and reach, because when I coauthored the *Network Centric Warfare* book, I hadn’t made these fine-grained distinctions in my mind (**Figure 21**). I was spending a lot of time focusing on the richness attributes, and I wasn’t able to describe the problem with these two axes.

What happens when you’ve got a network is that you can provide not only information reach but also an unprecedented degree of richness. In other words, if you are a platform driver, and all you have are your organic sensors, and you’re trying to keep track of what’s going on with your fellow warfighters with voice, you’ve got limited situational awareness. If you do that at night, then you complicate things. However, when you’re able to connect with a network you’re able to create a condition that you couldn’t get to before, which corresponds to shared battlespace awareness. You couldn’t get to it before in the same way that Amazon.com couldn’t exist before the Internet existed: shared battlespace awareness couldn’t exist before the network existed. When we talk about the information component that enables shared battlespace awareness, what we’re talking about is the ability to fuse information on friendly, potential, neutral, and adversary forces as well as the environment and display it digitally (**Figures 22 and 23**).

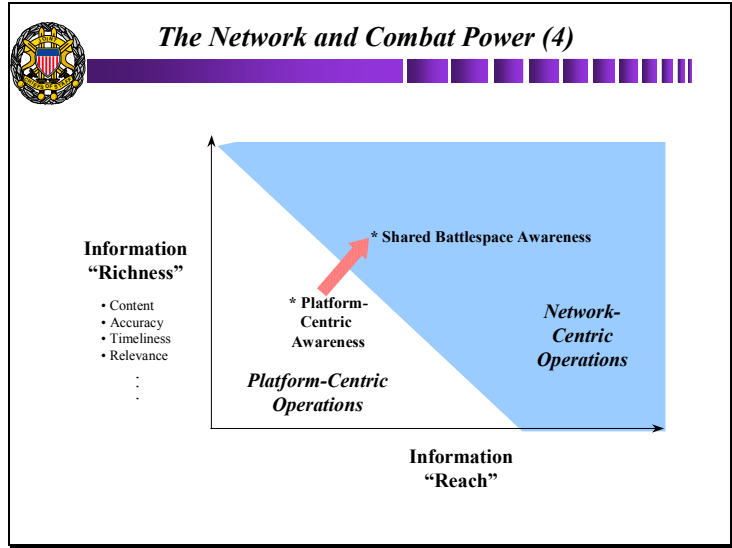


Figure 21

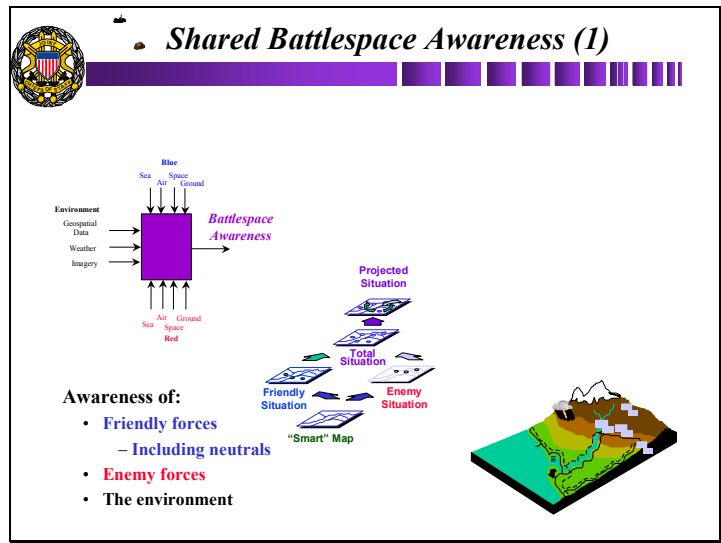

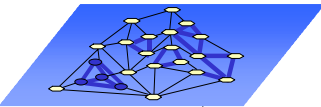
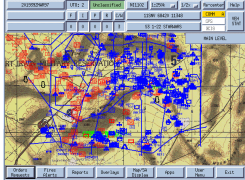


Figure 22

One of the key take-aways that I want you to leave the presentation with is that the customers say they want an operational picture with certain attributes, but when you go to the customer and say, "If you want this operational picture, then you need to buy this network," you get one of those deer-in-the-headlights looks. In other words, they don't understand it. It's like going to somebody and having him or her say, "I want to log on to the Internet but I don't want to buy a modem." If somebody did that you'd say, "You're ridiculous! You don't get it!" We face this same challenge. I've heard very senior four-stars say, "I want to see an integrated air picture but I don't want to buy the network." They've got a legacy mental model. They don't understand what the entry fee is for the information.

 **Shared Battlespace Awareness (2)**

- A network-centric force has the capability to generate shared battlespace awareness.

The generation of shared battlespace awareness requires the **robust** networking of the blue force.

Figure 23

Oettinger: Partly they may be stupid. There may be some other factors as well. Let me draw an analogy from the banking world.

One of the ongoing (and it has been ongoing for decades) problems in the banking world, which I think is analogous to this, is that every customer would very much like to know what's going on with all of his or her accounts in the bank. You can say that information technology ought to be able to do that. I don't know of any bank that is able to give you a total picture of all of the relationships. They're groping toward it, but you have savings accounts, trust relationships, certificates of deposit, et cetera. Now, why is that? Technology is part of it, but part of it is also that the trust department and the retail banking department, et cetera, each has its own various power base and one thing or another, and the folks don't necessarily want to have all that pulled together. There may be a little bit of an interservice issue. They understand perfectly well, but they would just as soon not have all that togetherness. This is true, for example, in spades in the intelligence community as well as in the military. There are, again, a whole number of electro-political factors at work.

Garstka: I agree with you, but the other side is that some banks have recognized that by fusing their information internally they get a much better picture of their customers and their risk situation than they did before. It used to be, as Dr. Oettinger pointed out, that your checking account information was in one database, your car loan was in another database, and your mortgage in another database, even if they were all at the same bank. The bank had very poor situational awareness of their customers.

Oettinger: Until the recent [1999] amendment of the Glass-Steagall Act,¹⁵ even if they wanted to have situational awareness they could not convey that information to you through one clerk, because it would have been illegal to provide information on an insurance relationship you might have had with them in the same breath as information on a banking relationship. This is one of

¹⁵The Glass-Steagall Act of 1932 (actually the Bank Act of 1933) in effect keeps banks from doing business on Wall Street, and brokerages from acting as banks.

the reasons why the banking industry lobbied for the repeal of the Glass–Steagall Act and the insurance industry fought it tooth and nail, and you have a semi-repeal that has altered the dynamics of the competition between those industries. I’m pointing this out simply to give you a sense of the dynamics at work here. Whether it’s banking and insurance, or Army and Navy, or the Central Intelligence Agency, the National Security Agency, and the National Imagery and Mapping Agency, there are very common institutional dynamics that lie behind this, and not just executive stupidity. Some folks don’t get it, but they may get it and it’s just better to say that they don’t get it than to say, “I don’t want to share this information with the guy next door.”

Garstka: When we talk about the value of a network, it’s important to understand that we have facts that support the combat power associated with a netted force (**Figure 24**). In these mission areas—maneuver, counter special operations forces, theater-to-air and missile defense, counter air, and strike—we’ve seen how networking the force, providing shared awareness and a capability for collaborating and synchronizing, is really key to the increased combat powers.

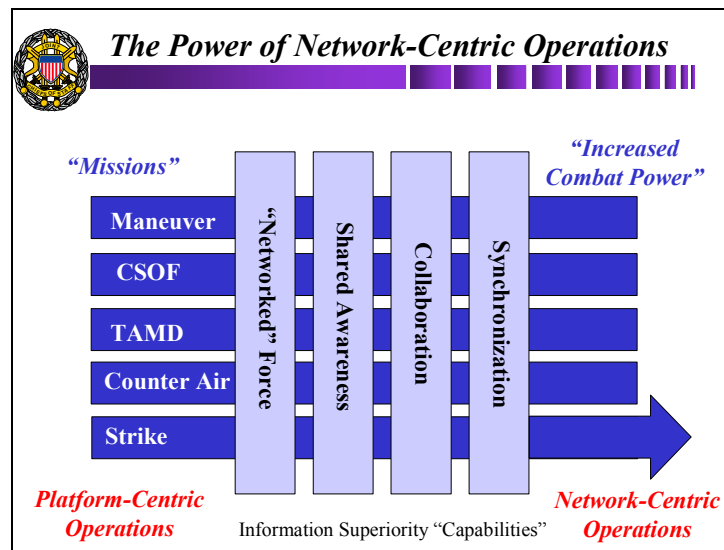


Figure 24

A previous graphic [Fig. 1] showed a lens of information superiority. We can see that this concept, which initially seems trite, turns out to be quite accurate. If you think about that lens as a composite lens that has a number of different sublenses, that’s what we see happening here. Again, if you’re interested in the details, I’d direct you to the *Network Centric Warfare* book, because it highlights what the force multipliers look like in key mission areas.

Oettinger: John was just telling me there is a third edition on its way. The second edition is in PDF format on the Web. The third is anticipated...

Garstka: ...probably in the next year. We’re just talking about it right now.

I’m going to spend the rest of the presentation talking about some details of the concept that General Woodward has introduced for the GIG (**Figure 25**). We really think about this as a reference model—as a way to describe the complexity associated with all the pieces for

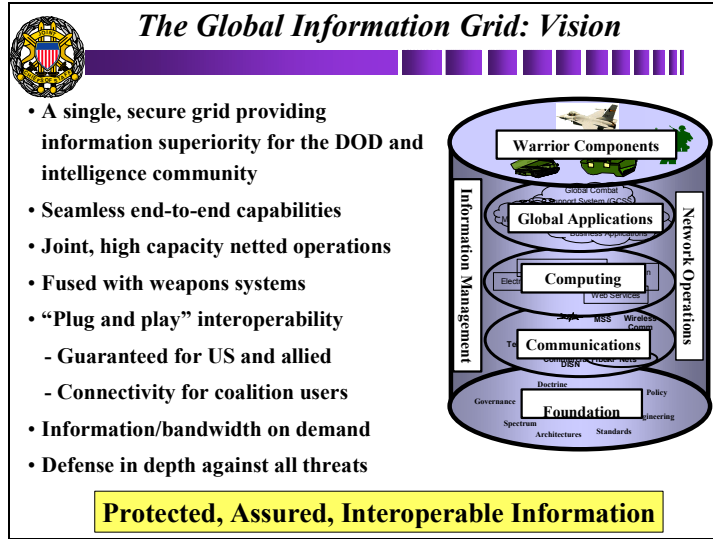


Figure 25

networking the force. I’m going to go through each of these constructs and provide some additional richness (to use the analogy) about what we mean when we’re talking about them. The desired point in progress is protected, assured, interoperable information. One of the things you want to be able to do is start from the customer and work backward. That’s what we’re doing when we talk about the warrior components (Figure 26). We mean the warrior’s understanding the specific needs for connecting the platforms to the network and understanding that the information these nodes consume is really key to generating combat power. If you believe that, then you have to start thinking about the grid as a weapons system, because if you don’t you’re going to marginalize your combat power, and when you go into harm’s way you’re not going to be able to depend on the network.

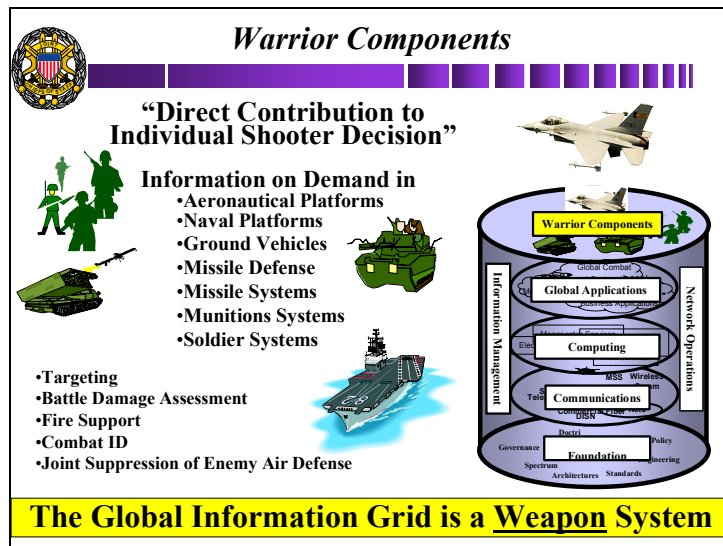


Figure 26

At the bottom, at the foundation layer, we see some things pulled together that are really important (**Figure 27**). Dr. Oettinger talked about policy, doctrine, and governance. These are key attributes of the grid. Some of this is really behind the scenes. If you think about why the Internet is successful today, there's a lot of policy, governance, engineering, and compliance going on. The Internet Task Force¹⁶ has been key to solving some of these interoperability problems. I would assert that until recently the senior leadership in the DOD hasn't appreciated that these are strategic issues. They aren't issues that we can afford to work at the margins. They're fundamental strategic issues on which we have to place a priority from the perspective of resources and intellectual capital.

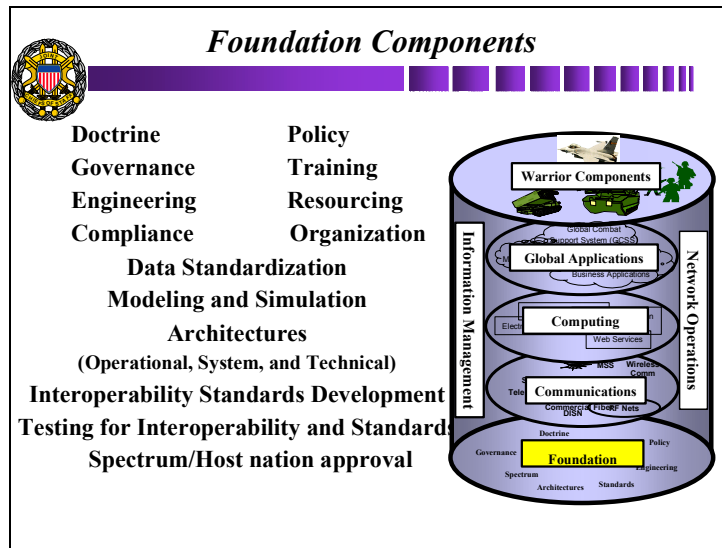
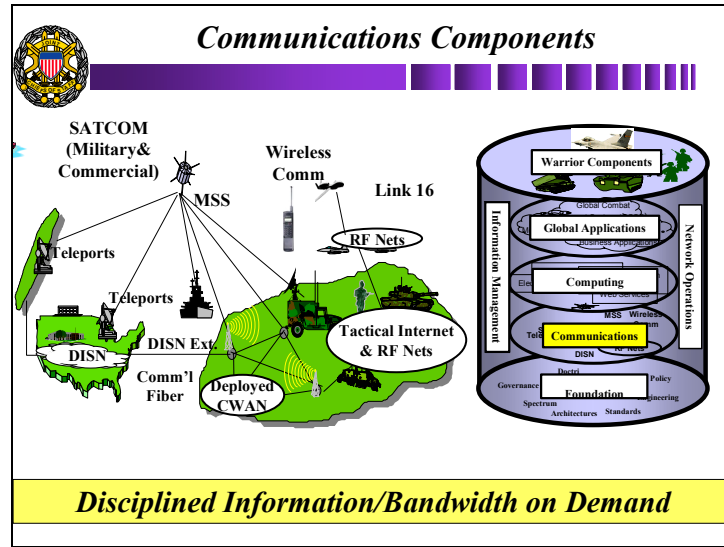


Figure 27

When we talk about the communications components (**Figure 28**) we're talking about a lot of different modes and modalities of information. We're talking about radio frequency [RF] communications, wireless communications, and satellite communications. We're talking about the types of backbones that the SIPRNet [Secure Internet Protocol Router Network] and NIPRNet [Nonsecure Internet Protocol Router Network] ride over. We're talking about disciplined capabilities for providing information and bandwidth on demand. This is a really tough problem. When you think about the excitement going on in the commercial sphere today, and about the whole issue of Internet over voice and being able to provide Internet capabilities to either Palm™-like devices or to telephones, you're seeing a desire to commercialize things we tried to do in the military for the past couple of years. In many cases, it's much easier in the commercial sector, because, for the most part, you can put down towers so you can operate in the RF domain. In our domain we basically have to move around. We've got to break things down. In some cases we have a harder problem, and in other cases we can see that just in the United States, because of subtle issues such as standards, one mobile phone won't talk to another. In Europe, with their

¹⁶This is, officially, the Joint Task Force on Computer Network Defense, established by the Unified Command Plan in 1999.



CWAN = coalition wide area network DISN = Defense Information Services Network MSS = mobile satellite system

Figure 28

GSM [Global System for Mobile communications] standards,¹⁷ if you buy a mobile phone it's going to operate pretty much with any provider, whereas here these standards mean that a phone that works with AT&T is not going to work with Cellular One. The roles of standards and governance are really key, and they have significant implications for making this type of construct work on the battlefield.

When we talk about computing components (Figure 29) we're talking about a broad set of attributes, from megacenters to data services to shared mapping services to electronic mail capabilities. There is a broad set of services and capabilities that falls under the rubric of computing. Similarly, when we talk about global applications components (Figure 30) we're talking about applications such as the Global Command and Control System [GCCS] and the Global Combat Support System [GCSS], which are the types of applications that the intelligence services employ and business applications that are key to the revolution in business affairs. This is one of the real reasons why the Navy is so excited about the Navy-Marine Corps intranet. They want to be able to bring their business applications on board. As the under secretary of the Navy has said, if the Navy can't do that and can't figure out how to work more effectively, they're going to have a problem, because their people are retiring and they're not able to attract new staff. This isn't just about technology. There is a close coupling to what you want to do with your intellectual capital.

There is a training component as well. People in J-6 have to deal with the challenge of applications that are deployed without dollars to train the force. These are really complex issues.

¹⁷GSM is an open, nonproprietary system that uses digital technology and time division multiple access (TDMA) transmission methods. It is the standard in the European Union.

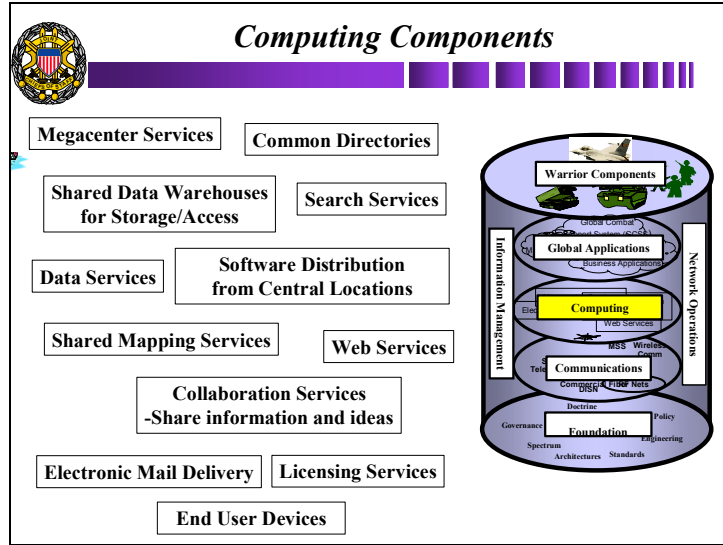


Figure 29

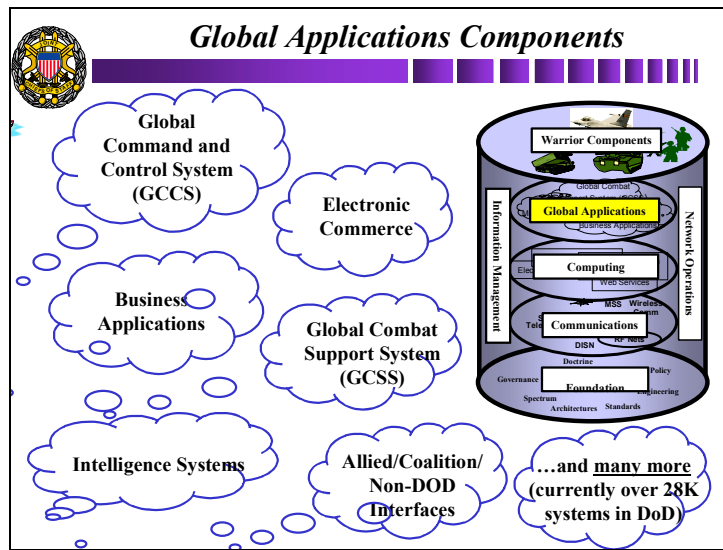


Figure 30

Student: How does it help military organizations to operate?

Garstka: For instance, anyone who has studied history can tell you that an army fights only as far as you can feed it. Military services buy many things from the commercial sector, such as foodstuffs, that they can buy less expensively via e-commerce. Fuel oil and petroleum can be bought more effectively with e-commerce. The whole business end of defense—the support end—is very amenable to the types of concepts that we see emerging in the commercial sector.

Information management [IM] is a very important attribute (Figure 31). Some of you may be familiar with the company MicroStrategy, which advertised during the Super Bowl and recently had a big blowup about its stock price and is being investigated by the Federal

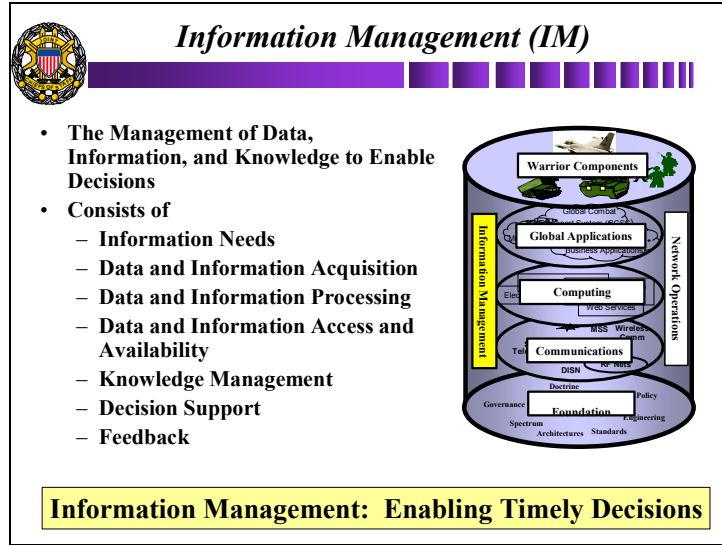


Figure 31

Communications Commission. They're talking about providing this sort of capability to individual customers. In other words, the customer can get tailored information; for instance, a phone message that says, "Your flight has been cancelled. If you would like to schedule another flight, press 1." Then it would say, "Do you want to do it at *this* time or at *that* time?" The ability to provide that information in real time is using information to provide real value for a customer. What we're seeing today is that this is a competency we don't have yet in the defense space, and it is one that we need to develop effectively.

When we talk about network operations (**Figure 32**), we mean being able to have situational awareness about what's going on in the network: where we potentially have a backup, or where nodes are malfunctioning and slowing down information. We want to be able to give the warfighter insight if he needs to provide intel information and there isn't enough bandwidth. That involves network management and the ability to manage information dissemination, link information assurance capabilities with your network operations, and have tools for on-line modeling and simulation. We're in the process of developing those tools today. We also have the capability for mission planning and trend analysis. In other words, if a contingency comes up, you can do the modeling and simulation and understand what the implications are of moving various satellite communications channels around to support the forces.

Oettinger: If I may make a link between this and a whole set of other issues, one of the questions that I hope comes to mind when you look at all this, given the immense complexity of it, is what happens if all this disappears on you, either because somebody put it out of commission or because the power failed, or whatever.

Student: Then we have symmetric warfare, which is a lot scarier than asymmetric warfare.

Oettinger: Yes, you have the possibility of everybody getting so scared that they nuke one another. This is an extremely important observation, and I want to draw you back to some of the literature and some of the thinking in the cold war. Things like the Moscow–Washington hotline and communications facilities for war termination as well as war fighting had an enormously

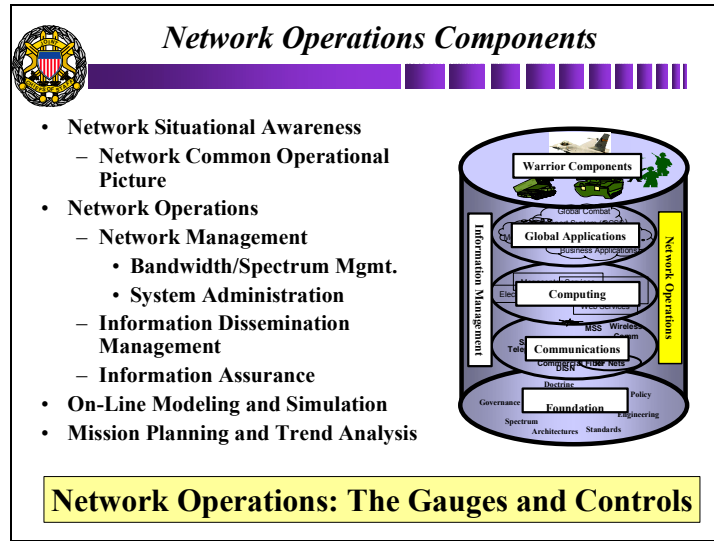


Figure 32

important role in the management of forty to fifty years of cold war for precisely that reason: the realization that the danger in this stuff failing might be much greater than the dangers inherent in its working. When it works, you have a chance of some limited objectives being attained by a limited application of means. That assumes a certain amount of rationality all around, which is not something that one can always count on but it is an enormously important problem. The reason I raise it is that discussion of it has seemed to disappear since the disappearance of the cold war. It strikes me that you should all remain very much aware of this, because keeping this stuff operating not only for ourselves but also for any potential adversary is as key an issue, to my mind, as it was in the Soviet-U.S. confrontation.

Student: How would we feel, or how should we feel, if a set of potential adversaries—other countries, people we look on as bad guys—were to get this? What sorts of things would we do? What strikes me is that there is a kind of symmetry to this. Perhaps we would pioneer it, other people would learn from us, and then they could do it.

Garstka: Regardless of how we feel about this, the technology is there, and we have very capable adversaries. Take the example of Wal-Mart. The technology was always there. Wal-Mart out-executed its competition. They recognized that the ability to operate in the information domain wasn't just a core competency, it was one of the most important core competencies.¹⁸ We are in the process of shifting from our existing mental model, which five years from now I will probably call a legacy mental model, to a new mental model where we recognize that understanding how to operate in this type of information domain is about combat power. The advantage that we have is out-executing an adversary. It's not just about the technology. It's about the people, it's about the process, it's about the doctrine, and it's about understanding how to overcome the organizational inertia that exists today that keeps the services from doing some of these things. These challenges have nothing to do with national culture. You can go to any armed forces in the world and you can see the same thing. I guess that's the good news.

¹⁸Wal-Mart's data mining initiative has greatly increased its dominance of its market space.

The other thing that's important to understand is that the network is about reach, and the richness is a function of your sensors. If you have better sensors, then you can do things with those sensors when they're connected to a network that you can't do otherwise. So, if we can outperform our adversaries, the platforms are still going to matter, but figuring out how to network those platforms is more important than ever before.

Oettinger: Let me pursue your point a little bit more. First of all, it's unavoidable. Throughout history every measure has been countered by a countermeasure, and the only question is how long it takes. Second, it's a mixed bag, because it's entirely conceivable that it's mutually advantageous not only to have them all around but also to have them interpenetrated, with each side having total knowledge of the other. If you again take the cold war analogy, I would argue that the fact that no nuke ever got fired in anger between the United States and the Soviet Union was in large part due to mutual distrust (as in Reagan's famous phrase, "trust but verify")¹⁹ and that the national technical means—satellites, et cetera—that provided both the Soviet Union and the United States with a detailed view of each other's capabilities essentially were an enormously important factor in keeping the peace for years.

Garstka: There was also the Open Skies agreement,²⁰ which originated during the Eisenhower administration but didn't get off the ground largely because we got satellites, which made it almost irrelevant.

Oettinger: It got off the ground, because after the U-2 incident both the United States and the Soviet Union realized that keeping space open was going to be a stabilizing element. That was a profound decision made in the Eisenhower administration. Even though it happened to fail with the shootdown of Gary Powers, it succeeded enormously when both sides realized that they were better off sharing space (at that time to the exclusion of the rest of the world, because it was purely a bilateral thing). It created a degree of stability for the period of the cold war that was really quite remarkable. In terms how much of a stabilizing effect this had, I haven't the vaguest idea. It may be something that you want to think about.

Garstka: Let me pull the thread on this with an analogy. Look at what's happened in the financial services sector, with individuals having access to on-line trading. The dynamics of the market have changed. The advantages that the institutional brokers used to have are being marginalized. Just having the information isn't so important as having knowledge. In other words, it's the combination of competencies in the information domain and competencies in the cognitive domain that give you the advantage. That's always going to be the case in warfare. It has always been about people. It will always be about people.

Student: Does that mean that you will be developing a network in parallel with this kind of process? Will you have to retrain people to think in network ways? In other words, the training of people has to parallel this technology development. I don't see network training going on.

¹⁹This phrase, which President Ronald Reagan was fond of quoting during disarmament negotiations in the 1980s, is a Russian proverb.

²⁰The Open Skies Treaty was proposed by President Eisenhower in 1955 to encourage reciprocal openness among participating states through overflights that would allow the signatories to observe one another's military activities and institutions, in an effort to foster confidence through what has come to be called transparency.

Garstka: I’m just going to use data links as an example. There is not a single service today that has completely equipped all of its airframes with data links. In the Navy, with the deployment of IT-21,²¹ you’re only starting to see new tactics, techniques, and procedures being developed. They have to have the network there and they’ve got to train people how to use the basics. Then they’re going to start figuring out how to do things differently.

Student: It’s going to come along eventually.

Garstka: Yes, but they need the insight you’re highlighting: that it’s not just the technology, it’s the people and the technology together that give you the payoff.

Oettinger: What’s new here? What’s new is that this is by far the best analysis of the impact of new technology that I’ve seen in captivity anywhere. What’s old about this? This is a parse of what is by now a fifty-year-old notion of information as a force multiplier, but it used to be that one mumbled “force multiplier.” “What does that mean?” Silence. This is a beautifully detailed, analytical expansion on the notion of force multiplier.

Having said that, and going back to his point about the importance of the people, I’ll take you back to World War II and the technology of radar. The Germans and the Brits and the United States had radar. The difference was in the use, which is precisely the point he has made about force multipliers. The British used radar effectively as a force multiplier. They used it to detect incoming bombers and concentrated their fighter planes where the bombers were coming in, denuding all the other sectors, but with reasonable comfort that if their radar didn’t see anything there wasn’t going to be an attack and they could simply multiply the effect of all the Spitfires concentrating on one sector. The Germans, with the same technology, used it as a kind of electronic Maginot line, as airplane spotters all around the periphery. It never dawned on them that they could use it differently. Likewise, the British bomber command never really understood what to do with radar. It happened that the leadership of the fighter command had the conceptual leap that they could use the technology to alter their tactics radically.

Garstka: The same thing happened with the Germans and Blitzkrieg. They were able to use several technologies, one in the form of the radio—mobile communications. We had a detailed discussion about this yesterday. One of the most significant factors in the early German success was what was going on in the cognitive domain, because these people had trained together, they understood how they thought, and they understood how they operated. Later in the war, as their forces got attrited, they weren’t able to share awareness. Even if they could share information, they weren’t able to share awareness in the same sense, because they didn’t have the same wiring of the cognitive domain.

Student: There are lots of writings out there now on this thing you keep calling the revolution in military affairs [RMA]. They do put some end-states on those processes, and it’s important to figure out where some of them started and stopped. Arguably, the current RMA is information based, and people are deciding where one starts and maybe the next one starts. But it is important to see where those are. What gets back to the whole policy and politics side of it is that this

²¹IT-21 (Information Technology for the Twenty-First Century) is a Navy initiative to ensure that naval forces achieve and maintain information superiority. It involves a reprioritization of command, control, communications, computers, and intelligence (C4I) programs to provide operating forces and the operational support infrastructure with a seamless command, control, and communications structure that is fully compliant with joint community standards.

technology is available to anybody out there, and if you study when those previous RMA periods started and stopped you will notice that it wasn't always the people who developed the technology who were able to put it to advantage. Again, there's the example of the French and the Germans and tanks.

Our concern is how to make sure we are the guys who take advantage of our own technology. A lot of it comes back to politics and bureaucracy and how you pay for it. You realize that a potential adversary could start this, because we don't have the industrial base that controls all that anymore. It could be the adversary who starts right now and catches up with us.

Garstka: I won't argue with that.

Student: Earlier in your slides [Fig. 26] you had multiple requirements for each of the platforms, each needing its own environment. They tried to deploy an airplane that satisfied the Navy and the Air Force, the F-111, and it ended up being something that nobody wanted. Is there a risk when you're trying to go from platforms to networking that the same thing will happen and that maybe you'll end up with something that doesn't really satisfy any of the customers?

Garstka: That's a very insightful question. I think one could say that if you don't understand the relationship between information and combat power you cannot spend your money efficiently. In other words, it would be very easy to spend money and not get combat power, in the sense that if you only spend money on the network and you don't spend money on training your people to use the technologies, and if you don't understand that it's the new tactics, techniques, and procedures that really allow you to leverage the technology, then you're building a white elephant. That's the analogy. The technology by itself is an entry fee. It's necessary but not sufficient. The sufficient conditions are what we just discussed.

Student: Are all the people who are trying to go from platform-centric to network-centric aware of that situation?

Garstka: No. That's what the NWC book's about.

Student: Buy the book!

Oettinger: There's plenty left for you to do.

Student: You could do a lot of research on this, how nice.

Garstka: What are some of the high-level attributes of the Global Information Grid (**Figure 33**)? When we put together desired operational capabilities for *Joint Vision 2010*, we highlighted capacity, information management, interoperability, assurance, and the key challenges of working with allied and coalition partners. These are attributes we want to be able to get for the grid. But when we look at what's going on in our own sandbox with respect to some key initiatives, this is how they fall out with respect to the components of the grid (**Figure 34**). What the grid reference model has done is given us the capability to sort things into bins, because before people talked about these things like apples and oranges. There really wasn't a coherent nomenclature for figuring out how they fit together and whether or not you're even balancing your portfolio.

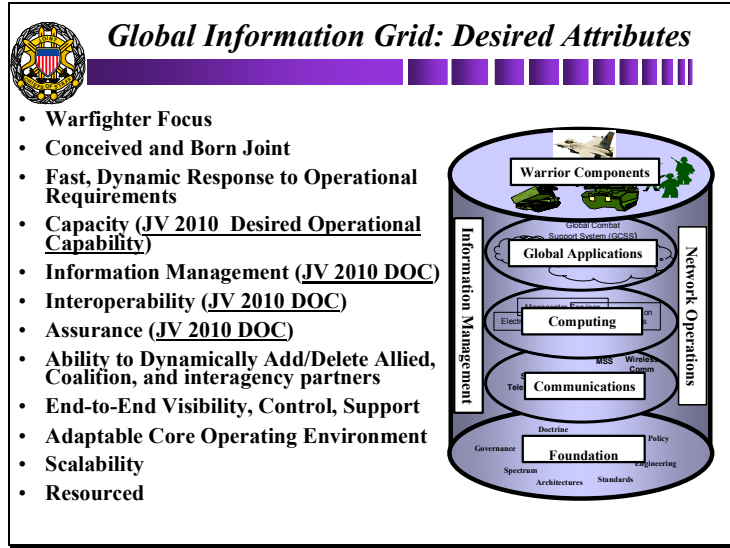
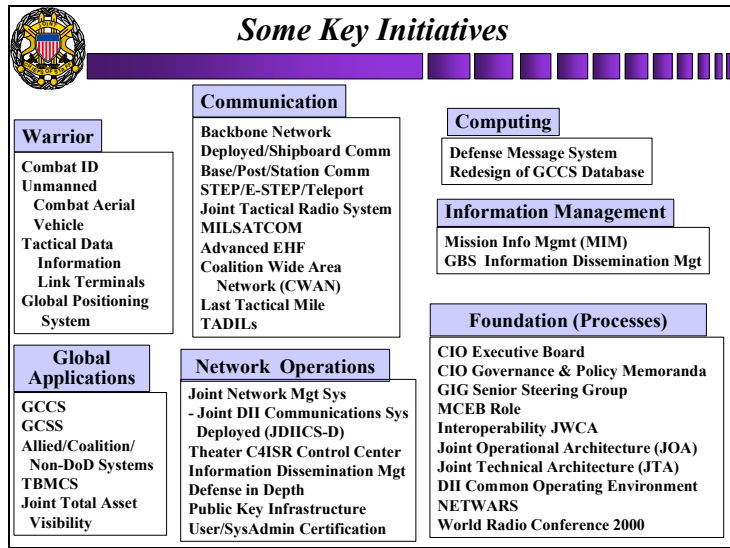


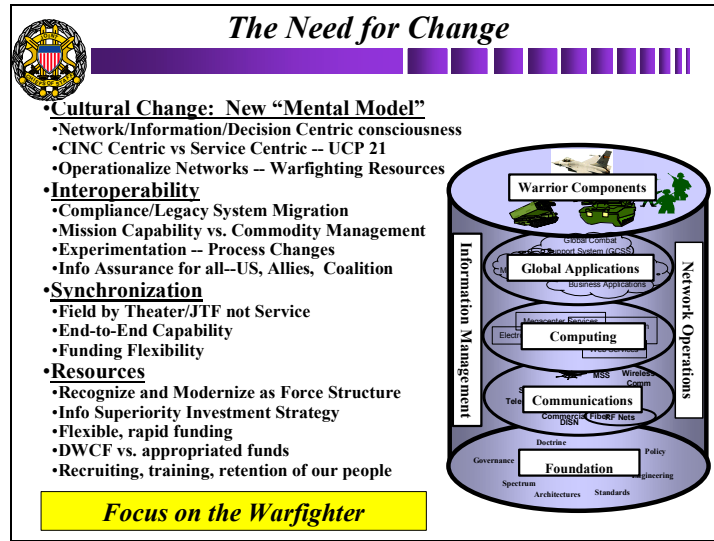
Figure 33



GBS = Global Broadcast System JDIICS = Joint Information Infrastructure Communication System JWCA = Joint Warrior Communications Architecture MCEB = Military Communications and Electronics Board STEP = Standardized Tactical Entry Point TBMCS = Theater Battle Management Communication System

Figure 34

As we've discussed for the past hour or so, it's not just about the technology. There is clearly a need for cultural change in the form of a new mental model that helps you understand the power of the network from a network-centric consciousness (Figure 35). The focus on the network is about understanding that the network allows you to do things in the information domain that you couldn't do before. It gives the customers—in this case the warfighter or sometimes the National Command Authority—the capability to make more effective decisions or to make decisions faster than an opponent.



CINC = commander in chief DWCF = Defense Working Capital Fund
UCP = Unified Command Plan

Figure 35

We have to recognize, of course, that we have some major challenges. We're a big company. Synchronizing deployments both by theater or in a joint task force [JTF] is important. You can't just have one service roll in with capabilities and not have them work from an end-to-end capability. One of the things that we're doing as part of the Quadrennial Defense Review is developing an information superiority investment strategy. We're trying to get that right. We've recognized that, as in all competitive endeavors today, recruiting, training, and retaining people are really important. If you don't have the right intellectual capital all the rest is a fantasy.

Oettinger: Again, where there is death there is hope. It may be that rotating and bringing in new people may be a better thing than having to deal with legacy mental models.

Garstka: People have looked at the RMAs and basically said that in many cases the pace of an RMA is a function of the attrition of the legacy mental model.

Student: It's not just keeping people, it's keeping good people. The way the commercial market is now, it's hard to keep good computer guys on the money we pay them.

Garstka: It's not just the money. The CIO of Wal-Mart has a seat at the table in the inner circle. In too many of the services the CIO equivalent isn't viewed as having a seat at the table. If you believe that this is a potential way ahead, that mindset has to change.

Student: Plus, the DOD used to be the place you went if you wanted to play with the new toys, and that's no longer true. That is unfair when you're looking at recruiting young folks who are in need of exciting stuff.

Garstka: Right. To attract those people we have to highlight what we're doing. If you look at the existing recruiting campaigns, you can't see that anywhere.

Pulling it all together, we are working on some procedural and policy issues (**Figure 36**). One of the most significant is the rewrite of a Chairman of the Joint Chiefs of Staff Instruction [CJSCI] dealing with the requirements generation process, which has highlighted interoperability

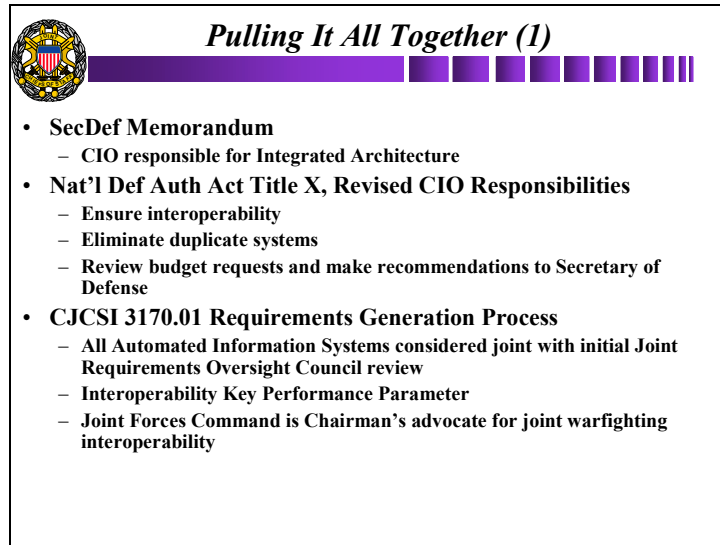


Figure 36

as a key performance parameter of all major systems. This is a big, big deal. I cannot overemphasize the importance of that development.

Oettinger: The Army might even change the slogan to “be virtually the best you can be.”

Student: I wouldn't doubt that if you put “land a career” in the commercial, you might attract some.

Garstka: Parts of J-6 are working very closely with Joint Forces Command to put together a capstone requirements document for the GIG (**Figure 37**). This is, at least, a shot across the bows in terms of helping audiences understand at a high level the relationship between components, capabilities, what's enabled, and what some of the outcomes are (**Figure 38**). As I pointed out previously, some of the details about combat power at the individual mission levels can be found in the NCW book.

Oettinger: There is a paper by Charles Popper relevant to what he's been talking about: CIOs and the seat at the table, and the relationship between the technology, the processes, and the business end results.²² You can find it on the Program on Information Resources Policy's Web site. Those of you who are seriously interested in this topic might find it very useful to read that paper in conjunction with John's presentation.

Garstka: Albert Einstein once said, “You can't solve today's problems with the same kind of thinking that created them,” and General Woodward makes that point in several of his presentations. What I think you've seen today is some of tomorrow's thinking. You're starting to see some of the foundations for a new mental model to help us deal with the complexity and to make some progress.

²²Charles Popper, *A Holistic Framework for IT Governance* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-00-1, January 2000, [On-line]. URL: <http://www.pirp.harvard.edu/pubs/html>)

Pulling It All Together (2)

- **Joint Requirements Oversight Council (JROC) directed GIG Capstone Requirements Document (CRD) be written**
 - Create a single overarching requirements document
- **Joint Forces Command is CINC Lead**
 - Action Officer meetings 17 Dec 99 and 11 Jan 00
 - CRD Development Meeting 4-6 Apr 00
 - CRD to JROC Requirements Panel (O-6 level) July 00
- **C/S/A, OSD, Intel Community participation**

C/S/A = CINCs, services, agencies OSD = Office of the Secretary of Defense

Figure 37

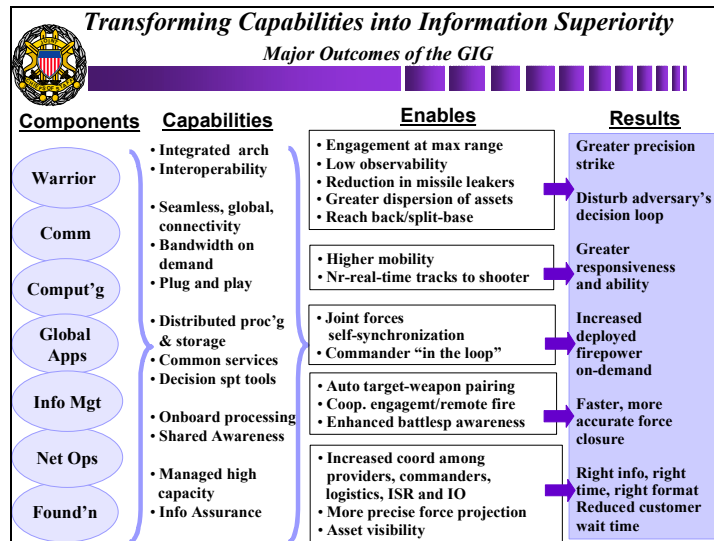


Figure 38

Of course, the way that you recognize the new elite is by the way they mark themselves. This is one of General Woodward's favorite tattoos (Figure 39). It is our bottom line: if you want to get to a network-centric environment, you've got to make the Global Information Grid a reality and a priority.

That wraps up the formal presentation. I would be happy to take any additional questions that you might have.

Student: Earlier in the briefing you started talking about information dominance in terms of relative information advantage. Actually, you made it relative in terms of sort of a polar situation; that is, you had blue wanting to expand and at the same time to diminish red's information space,

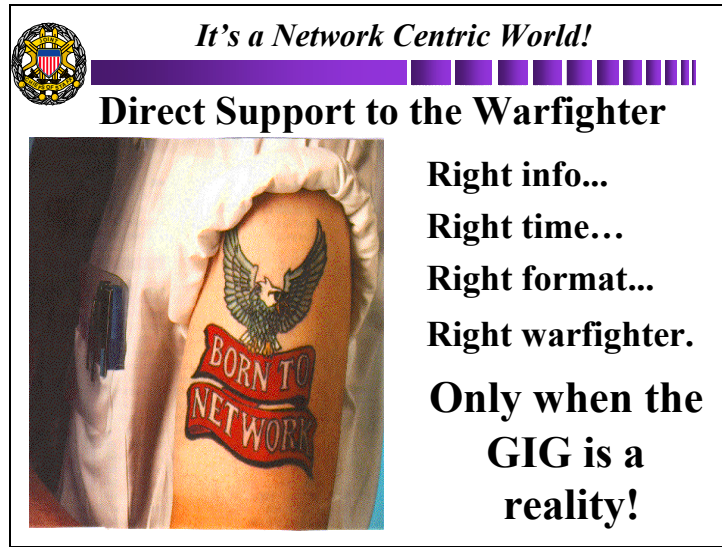


Figure 39

and vice versa [Figs. 4, 5, and 6]. There's a third party in this, and that's the public domain. It's a third party that we find is incredibly important in trying to achieve the national interests of the United States. How are we going to try to dominate the information in the public domain as well?

Student: Ask the admiral who is sitting there.

Garstka: In Figure 6, we identified that it was n -sided, and perhaps we've got to put in a third cube that represents the public. That would be a very good addition, because we realize that's the case.

Student: I don't just mean the U.S. public; I also mean the international public that really shares this public domain of information.

Garstka: Some interesting things have happened in terms of the role of the network in politics. There was an article in the paper about how the Internet was used in Korea to distribute information on some potential candidates that the papers, because of their leanings, weren't willing to share.

Student: I went through a seminar at Air Command and Staff College and I learned about psyops, our little mutant DOD effort to control information in the public domain. Over at the [Harvard] Yard, one of the things I've studied is Chinese propaganda, which is much more developed than our own psyops capability but is still not all it could be. It's still somewhat ham-handed. I also got an MBA some years ago and I took marketing classes. Those marketing guys know how to affect information in the public domain. Yet, as far as I can tell, our psyops people don't ever go to them. They've got an enormously well developed set of information doctrine procedures, if you will, about how to control that information space.

Garstka: You highlight a very important point. My coauthors and I have been criticized at length from some quarters for bothering to talk about business. "What are the relationships between business and warfare?" One of the problems is that very few people who spend any time in warfare have spent any time in business. The chief executive officer of Wal-Mart said, "I waste

50 percent of my marketing budget. I just don't know which 50 percent it is." That's about friction. That's about fog. Friction and fog are universal attributes of human behavior. They're exacerbated on the battlefield. There has been very little dialogue. Part of it is just because of the intellectual hubris. There just isn't an appreciation for what other individuals and other domains can bring to bear. If you think the issue with marketing is bad, until people have been deployed as part of a joint task force or worked on the Joint Staff, there is very little appreciation for the competencies of the other services, let alone competencies outside that domain and in commerce.

Oettinger: It isn't completely a desert. Just a few months ago, the intelligence people of the Marine Corps took themselves over to Goldman Sachs for training. There are people who are willing to learn from somebody else.

Student: There has to be a lot of thinking on the legal side when you start talking about controlling the public domain, although almost certainly we will build that bridge. All I'm saying is that you've got to be careful when you try it.

Student: Of course. Just the word "propaganda" makes an American shudder, yet it's interesting that the word in Chinese carries none of the negative connotations that it carries in English. In English it reminds us of Hitler, Nazism, government oppression, and control; bad things. All it means in Chinese is "information from the government," which could be Marine Corps recruiting. All those commercials about "Be all that you can be" are propaganda according to the Chinese definition.

Student: Your translation is wrong. Propaganda is "publicity."

Student: So you have a ministry of publicity?

Student: The Americans have been much more successful.

Student: When you talk about procuring systems jointly, it becomes a super-joint thing and then an executive jointness, and you're looking at systems that share intelligence between the military intelligence communities, and then it starts going closer and closer to local law enforcement stuff. There's definitely a point in there where you have to start looking at what it does to you legally and how you do that.

Student: Of course, the last situation we want to get into is a party using government instruments of information to preserve its dominance of the political structure, and I think that's what we're all so scared of. At the same time, we sometimes get rings run around us in operations overseas, simply because we're not working in the public information space.

Garstka: Part of it is that it's not viewed as a warfighting competency. That's a shortcoming of the war colleges. The place where that should be happening is at the war colleges.

Student: I suppose it's beyond our consideration here, but sometimes I think that apart from the Department of State, which basically just deals with diplomacy, the DOD is the "all other" on executing the national interest—not just warfighting, but all other missions, whether they're humanitarian missions overseas or peacekeeping missions or...

Oettinger: That is a grossly government-centric and navel-contemplative view. There are all those nongovernmental organizations, all those editorials, all those Peace Corps people, all those multinational corporations, and so on. One of the arguments that I participated in throughout the

cold war (and it was a piece of received wisdom in intelligence) was that we were working under this enormous handicap as an open society in contrast to the closed society in Russia, and they could learn so much about us and we had such a hard time penetrating the Kremlin. I thought and argued for years that it was bullshit, and some of the evidence from KGB²³ folks since 1990 has corroborated some of this. They had a much harder time, because with the cacophony of voices that come out of the United States, including a zillion nongovernmental statements, we generate an amount of white noise and disinformation that the KGB could never have enough budget to come close to deciphering. That is no ground for complacency, but it means that your statement that we are limited to the resources of the State Department and that the DOD is “all other” neglects the whole rest of the scenario.

Student: I guess what I’m saying is, if you accept that the United States ought to be playing in the public information space in a focused way, not a haphazard way, then the question is: What is our organization for actually doing it? The spokesman at the State Department? The spokesman at the DOD? Apart from that, there’s not much there.

Student: What would be an example of the government operating in the public information space? What would that include?

Student: Are you talking about our own public, or are you talking about overseas?

Garstka: It’s the same, because whatever we provide to our own public ends up being known abroad.

Oettinger: His point is that providing disinformation abroad is not the same as providing information at home.

Student: My point is you can’t have it both ways. You can’t tell your domestic public one thing and tell the overseas public another. The Chinese try to do that and frequently it bites them.

Oettinger: That’s the main reason for not doing it.

Student: You have to see this public information space worldwide as being a single space.

Student: Now it is. With the Internet that can happen.

Student: You definitely have an interest in what goes on in that space.

Student: An example would be the daily briefing during Desert Storm, where the J-3 and the J-2 got up and said, “This is the conduct of the war.” Saddam Hussein’s guy would get up every once in a while and nobody would listen to him, because he didn’t have video. It wasn’t cool. We were able to dominate the public information space in Desert Storm, I think, because Saddam Hussein was so bad at it.

Oettinger: Also because Mike McConnell is a hell of a good actor.²⁴

Student: He was. The J-3 guy was pretty good, too. But we’re not always going to be up against adversaries that are so incompetent at operating in that public space.

²³Komitet Gosudarstvennoi Bezopaznosti; the Committee for State Security of the former Soviet Union.

²⁴Rear Admiral John M. McConnell was the J-2 [director of Joint Staff intelligence] during the Gulf War.

Oettinger: We have ten more minutes left of our visitor’s precious time, and I suggest that we spend it wisely. What would you want to have said as John Garstka that wasn’t there in the words of General Woodward? What’s a key insight that you haven’t had time to present so far?

Garstka: I didn’t get to some of the facts and constructs associated with network-centric warfare that are in the book. There are some real insights there. If you think about the slides that had richness and reach [Figs. 10, 12, and 21], the exciting things that the services are doing can be understood as vectors that have different richness and reach components. For instance, when you look at what the services have done with Link 16, it’s about moving in one direction (**Figure 40**). If you look at what the Air Force did with their Joint Expeditionary Force experiment, it’s about moving in another direction. When you think about some of the things that happened during Operation Allied Force, we were operating way out here at the tactical level.

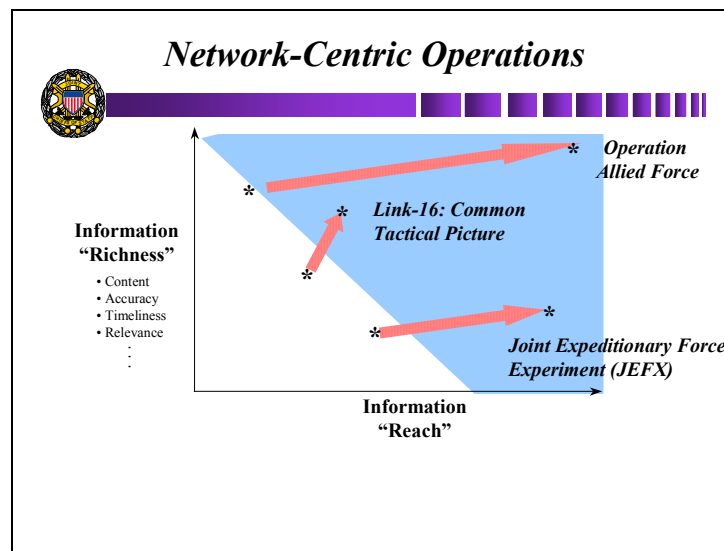


Figure 40

A year ago (and you will even see this in the NCW book), we had different vignettes. We didn't have a mental model for giving what I call the elevator speech. In other words, with this mental construct, I can now say, "Okay, Navy, you're operating up at full-dimensional protection. Army, you're going in the direction of dominant maneuver. Air Force, you're focusing on using the network to do precision engagement". All the services are making the shift to network-centric operations, but they're doing it differently. Instead of saying that one way is better than the other, you can just say they are all doing the same thing, but in the past we couldn't communicate that clearly and unambiguously. Now we can do that much more effectively. I think that's a significant development.

Student: Is the GIG a way of harmonizing all the separate network-based operations and bringing in the environment for everybody to share? They didn't that have before. They were all going about it in different directions. Now the GIG has the common environment for everybody to play in.

Garstka: The objectives are to be able to provide a common, joint environment and to recognize that there are certain things you need to be able to do at the joint level to make this work, because there is no such thing. If you have a service that depends on satellite communications [SATCOM], SATCOM is a joint asset, and it's controlled jointly. Some of the services would like to think that they generate combat power independently, but anybody that's within strike against fixed targets is dependent on national capabilities and comms capabilities that they don't own. So there is a shared network out there, but we haven't figured out how to share our toys fully. The GIG is about recognizing that it has to be a shared network. We have to treat it as a shared network, and we have to develop a rule set that we all agree to.

Oettinger: That need not imply uniformity of behavior. That's the point he was making: within that framework, different folks are applying it differently. A good analogy on that is the operation of the classical telephone network. Standards, as John has pointed out, are enormously important in enabling you to talk from here to Timbuktu, but what's marvelous about the phone network is that there is not the slightest constraint about the nature of your conversation. I think we are not quite so comfortable in the data realm because of its greater complexity, having on the one hand the capability to do anything with anybody but, at the same time, being able to have the substance be whatever is dictated by the circumstances and whoever is talking and whoever is listening and so on.

Student: That means that the GIG knows what's best when there is not too much politics interfering in the process. It lets these separate activities continue, because they do serve a service-level purpose.

Oettinger: But when they do want to interact, they are able to do so.

Student: Provided they have the standards.

Garstka: The standards have a strategic role. Once you have the standards right, then people want to operate with those standards, and they have the flexibility to do that. In many cases we're not at a point now where we can agree on the standards.

Oettinger: Sir, we are deeply in your debt, your family's, your ear's, and so on. Thank you very much. Here is a small token of our large appreciation.

Garstka: Thank you very much.

Acronyms

C4	command, control, communications, and computers
CINC	commander in chief
CIO	chief information officer
DOD	Department of Defense
DOTMLP	doctrine, organization, training, manpower, leadership, and personnel
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GIG	Global Information Grid
GSM	Global System for Mobile Communications
IA	information assurance
IO	information operations
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
IT-21	Information Technology for the Twenty-First Century
JCS	Joint Chiefs of Staff
JROC	Joint Requirements Oversight Council
JV	Joint Vision
KGB	Komitet Gosudarstvennoi Bezopaznosti; the Committee for State Security of the former Soviet Union
psyops	psychological operations
RF	radio frequency
RMA	revolution in military affairs
SATCOM	satellite communications



INCSEMINAR2000



ISBN 1-879716-74-7