

**INCIDENTAL PAPER**

**Seminar on Intelligence, Command, and Control**

**DISA and NCS  
Harry D. Raduege, Jr.**

**Guest Presentations, Spring 2001**

C. Kenneth Allard, Cheryl J. Roby, Nicholas Rostow, Richard P. O'Neill, Harry D. Raduege, Jr., Thomas S. Moorman, Jr., Thomas R. Wilson, James M. Simon, Jr., Toshi Yoshihara

**September 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](mailto:pirp@deas.harvard.edu) URL: <http://www.pirp.harvard.edu>  
ISBN 1-879716-76-3 **I-01-3**

September 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)  
NMC/Northwestern University  
PDS Consulting  
PetaData Holdings, Inc.  
Research Institute of Telecommu-  
nications 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

## DISA and NCS

Harry D. Raduege, Jr.

April 19, 2001

---

*Lieutenant General Harry D. Raduege, Jr., is director of the Defense Information Systems Agency [DISA] and manager of the National Communications System [NCS]. As director, he leads a worldwide organization that plans, develops, and provides interoperable command, control, communications and computers [C4] and intelligence systems to serve the needs of the president, secretary of defense, Joint Chiefs of Staff, combatant commanders in chief [CINCs], and other Department of Defense [DOD] components under all conditions ranging from peace through war. As manager, he is responsible for planning and provisioning national security and emergency preparedness communications for the federal government under all circumstances, including crisis, emergency, recovery, and reconstitution. General Raduege entered the U.S. Air Force [USAF] in 1970 and has worked his entire career in the areas of C4, space, and information operations. He has served in command, operations maintenance, engineering, plans, budgeting, and readiness positions at every organizational level, from detachment through major command. He was selected for the Air Staff Training Program and served in the Directorate of Command, Control, and Communications at Headquarters, USAF. Prior to assuming his current position, he directed command control systems for Headquarters, North American Aerospace Defense Command, and U.S. Space Command [USSPACECOM], and communications and information at Headquarters, Air Force Space Command. He also served as the chief information officer for all three commands. General Raduege received a B.A. degree in education (mathematics) from Capital University, and an M.B.A. from Troy State University. His major awards and decorations include the Distinguished Service Medal, the Defense Superior Service Medal with oak leaf cluster, Legion of Merit, Defense Meritorious Service Medal with oak leaf cluster, Meritorious Service Medal with five oak leaf clusters, Joint Service Commendation Medal, Air Force Achievement Medal, and Joint Meritorious Unit Award with four oak leaf clusters.*

---

**Oettinger:** You have all read General Raduege's biography, so he needs no further introduction. He has a presentation of about thirty or forty minutes but has declared that he would be willing to take questions as he goes along, and thereafter he is open to any other discussion. So saying, sir, we're glad to have you with us.

**Raduege:** Thank you, sir. It is a great pleasure for me to be here with you today. This is my first trip up here, so for me this is a tradition, responsibility, and opportunity that I haven't had the pleasure of experiencing before.

I have prepared a presentation for you today. The nature of information technology [IT] is changing very quickly in the world around us today, so these are all fairly new charts that I have put together with my staff. I wanted to make sure that I got some specific points out to you within the time constraints, because this business is so all encompassing, as I think you'll see. However, this is not one of those scripted presentations that I have given repeatedly, where I can just stand up and make sure that I hit on all the key points. I want to try to get through this prepared presentation so that we have time for extemporaneous dialogue, but I also want to take questions during the talk.

Communications continue to be a critical tool for deployed military forces. Admiral Dennis C. Blair, the CINC of Pacific Command [CINCPAC], really drove home a strong point about the power of information when he said: "Information translates directly into power... having the right forces in the right places at the right times and being able to support them." That is a key point, and an underlying principle for this presentation.

The organizations with which I am now associated have a proud past and a very exciting future (**Figure 1**). As you can see, we show two different organizational seals at the top of this slide: DISA on the left, and the NCS on the right. I'm what we call in the military "dual-hatted" as the director of DISA and the manager of the NCS. DISA is the keeper of what we currently call the Global Information Grid [GIG] for the DOD, and we develop and support C4I [command, control, communications, computers, and intelligence] for the National Command Authorities. On the other hand, the NCS assists in exercising emergency communications for the federal government during crises or emergencies, such as a terrorist attack or natural disaster.

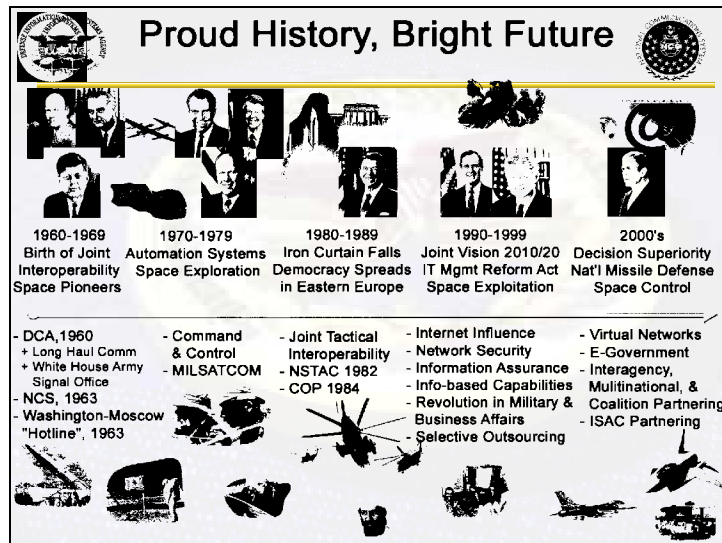


Figure 1

As you can see from this chart, we have changed over time. What began back in 1960 as the Defense Communications Agency has evolved into today's DISA. A few years later, our sister

organization, the NCS, was born in the aftermath of the Cuban Missile Crisis. I'll discuss the NCS in more detail later in my presentation.

As DISA has evolved, so has our mission. Initially we provided telecommunications management and direction, and we still do today. But more than that, for our information services support, we provide inherent joint interoperability, assured security, and overall best value. These constitute the core of our contribution to our customers—the CINCs, the military services, and the defense agencies.

We are witnesses to a new way of doing our mission—a revolution in military affairs fueled by *Joint Vision 2020*,<sup>1</sup> which was written by our Joint Staff in the military, and a revolution in business affairs, driven by the Defense Reform Initiative.<sup>2</sup> DISA recognizes the importance of these twin revolutions, and uses them to leverage technological change. My presentation will touch on some of these technological benefits.

I believe our future is indeed bright—not only for us but also for our customers and strategic partners. We have embraced today's Internet influence and we're moving toward e-government, Web-enabled applications, and virtual networks. But the digital world is not always safe, so network security continues to be a constant priority. We see a future for DISA that emphasizes interagency, multinational, and coalition partnering. We are also partnering with America's greatest treasure—American industry.

First, here is a quick overview of DISA's global presence (**Figure 2**). We have DISA employees at all these locations, and we now have many new missions with fewer personnel. As you can tell, we are not only performing traditional communications missions, but we're also deploying along with our nation's other military forces and engaging in new missions and initiatives. Despite manpower reductions, we have picked up the information assurance [IA], electronic commerce, and Office of Spectrum Analysis and Management missions. Since 1993, our personnel strength has dropped by 40 percent. At the same time, we've increased DOD's communications and computing volume by 5,400 percent. Certainly, these have been eight years of dynamic change!

**Student:** Could you briefly distinguish between information superiority and decision superiority?

**Raduege:** “Information superiority” was what we talked about in *Joint Vision 2010*,<sup>3</sup> as giving people enough information and the right information to be superior over a foe. What we have found out, though, is that we can inundate people with information. It's almost like your e-mail when you come home and discover you've got 150 messages. Holy Moly! You've got all the information in the world, but do you have time to fuse it in your own mind or to assimilate what it means? When you're trying to make decisions quickly and in a timeframe that's critical in some cases, what you'd rather have, instead of just information superiority, is “decision superiority.” Decision superiority tends to be that next layer up, where you've taken that information

---

<sup>1</sup>Chairman of the Joint Chiefs of Staff, *Joint Vision 2020* (Washington, D.C.: U.S. Govt. Printing Office, June 2000).

<sup>2</sup>Secretary of Defense William Cohen initiated the Defense Reform Initiative in 1997 to revolutionize business affairs within the DOD by incorporating lessons from the private sector.

<sup>3</sup>Chairman of the Joint Chiefs of Staff, *Joint Vision 2010* (Washington, D.C.: Office of the Chairman of the Joint Chiefs of Staff, 1996).

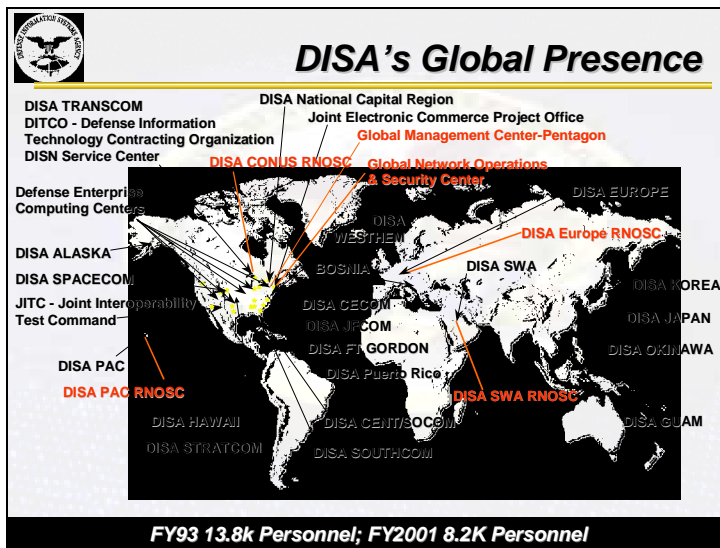


Figure 2

superiority and “just the facts” and somehow deciphered it into more meaningful information that will help you make the right decision.

**Student:** Would it be correct to see decision superiority as the next evolutionary step for information superiority?

**Raduege:** It is, and that’s why information superiority was emphasized so much in *Joint Vision 2010*, but, then, decision superiority was emphasized more in *Joint Vision 2020*. It has been an evolution in that case. You’re absolutely right. One of my bosses said not too long ago, “You know, Harry, before we move on to decision superiority, we still need to have information superiority,” and so that hasn’t decreased in importance. We still need to work on information superiority, because we need that to progress to decision superiority. There’s work to be done in both areas, but decision superiority is sort of a next step up.

**Student:** In that context, information superiority is still a core competence of the Air Force, but what about decision superiority? When you start trying to figure out who’s really doing it and what you’re leveraging, that would make a difference.

**Raduege:** It’s evolutionary thought. Obviously, I have ties to the Air Force and I know the information superiority piece, but also I have great ties in the joint domain. I have fourteen years of joint time now, and I think that through the Joint Staff we have evolved to “information superiority is good, but it’s not everything.” We need to progress to decision superiority, because the Joint Staff is thinking more along the lines of a joint task force [JTF] commander who has a huge amount of information coming in from all the military services and agencies. Each service could have itself pretty much optimized, but what the joint commander needs is somehow to fuse all of this into a clear picture in order to make the right decision.

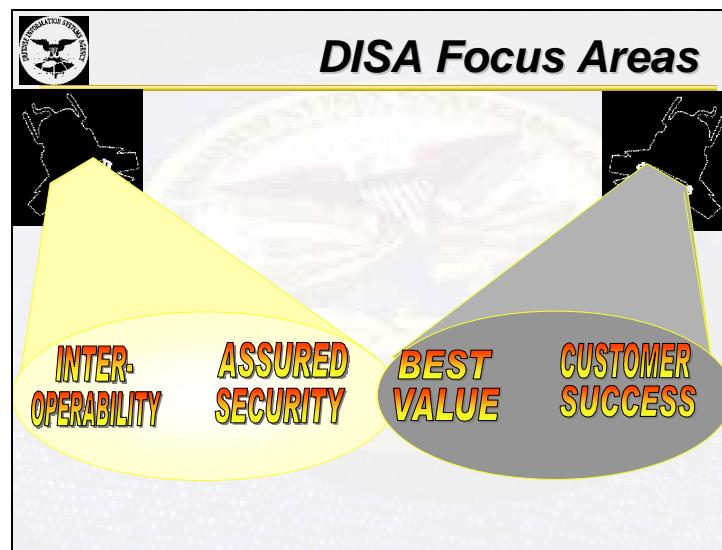
**Oettinger:** If we return to basic principles, in the O-O-D-A [observe-orient-decide-act] loop, the notion is that information is a means to an end, and the end is making good decisions. That means sweeping away some confusion. In other words, “information per se, so what?”

**Raduege:** That’s right. It’s making the right decision that counts. A lot of times, your decision is time critical. In other words, “Mr. President (or “Mr. CINC”), you have three minutes to make a decision,” and the information keeps flowing in. At a certain point, you can have all the information and there’s a whole other pile coming down the hallway at you or coming up on your computer screen, but you’re going to have to make a superior decision based on what you’ve got, in the limited time frame in which you have to make a decision.

**Oettinger:** I’m glad you brought that up. Some of you picked up that theme in your reading in Snyder,<sup>4</sup> but some of you didn’t.

**Raduege:** Not everybody in the Joint Staff and the services is working in perfect, cohesive unison, so when someone writes doctrine, it may take a while for somebody else to catch their doctrine up, because doctrine tends to take time. Most of us know what we’re talking about here. We know when we’re getting buried under information, and that we’ve got to make the best decision we can based on the information we’ve got. So we want to have superior information, but we also want to make a superior decision.

Let’s move on to DISA’s value-added focus areas (**Figure 3**). DISA’s “Job One” remains support to our nation’s warfighters across the entire spectrum of conflict. To achieve this, we must place additional emphasis on supporting DOD decision superiority. This means we must support the warfighters, DOD’s support structure, and other, seemingly growing mission areas such as humanitarian assistance, peacekeeping operations, consequence management, and disaster relief. Certainly, information is the catalyst in our overall decisionmaking process. We help DOD achieve decision superiority by focusing on four key elements: joint interoperability, assured



**Figure 3**

---

<sup>4</sup>Frank M. Snyder, *Command and Control: The Literature and the Commentaries* (Washington, D.C.: National Defense University Press, 1993).

security, overall best value, and customer success. I understand you want me to concentrate on interoperability and assured security today, but all four areas are equally important to DISA's mission.

Let me quickly cover all four of DISA's focus areas, and then we'll focus on interoperability and assured security. First, joint interoperability. Today, synchronized action across the battlespace depends on joint interoperability. It must be integral from the start—not an afterthought left to the JTF commander in the heat of battle.

Second, assured security. This means protected communication, free from service denial, interception, and modification. Our communications must be trusted, and security must be built into all products and services.

Third, best value. This involves up-to-date technology and increased capability at a decreased cost. DISA services bring inherent interoperability and security for the price—that's where "best value," not necessarily "lowest cost," comes in. There is a difference between the two, and you in the academic area know what that means.

Our fourth focus area is customer success. If our customers aren't satisfied, we're not doing our job.

When I first arrived at DISA, one of the first things I did was to read our charter, DOD Directive 5105.19. I was surprised to find the word "interoperability" cited thirteen times throughout this document. Here you see just a few of the spots where interoperability is mentioned (**Figure 4**). Joint interoperability is one of our core mission areas, and we understand the importance the warfighter places on it.

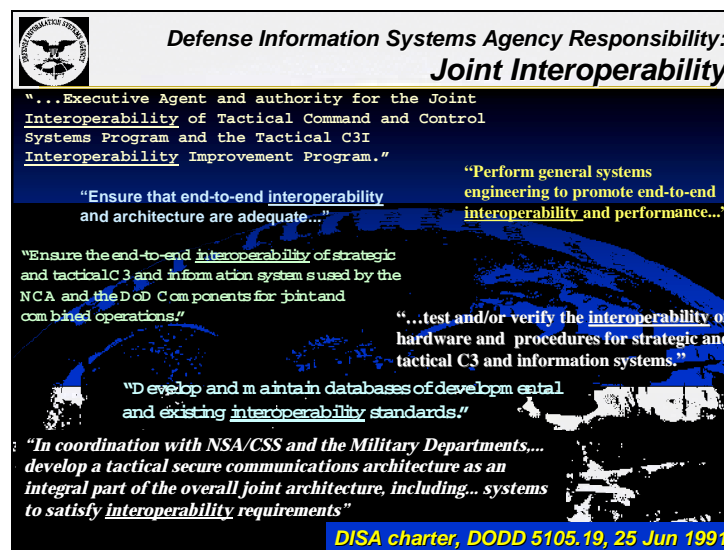


Figure 4

Standards are crucial to achieving this joint interoperability. But just as important, for standards to work, they must be followed. We've found that one of the most powerful sets of standards for DOD information technology is the Defense Information Infrastructure Common Operating Environment, or what we call "DII COE." The DII COE is the cornerstone of the



DOD's command and control [C2] and combat support computer software. It provides an environment of interoperable "plug-and-play" segments in which common, reusable infrastructure and applications across information systems help achieve interoperability goals. The current "short" list of systems using or moving to the DII COE includes forty-seven systems in the Army, thirty-five in the Navy, Marine Corps, and Coast Guard, twenty in the Air Force, and twenty in joint intelligence (Figure 5). This is a tremendous success story when you think about it.


 <b>Systems Using or Planning to Use the DII COE</b>			
Army	Navy/Marines/CG	Air Force	Joint, Intel
<ul style="list-style-type: none"> <li>• AALPS</li> <li>• ACGS</li> <li>• AFATDS</li> <li>• AMBISS</li> <li>• AMDWS</li> <li>• AMDPCS</li> <li>• AMPS</li> <li>• ANGSC-52</li> <li>• ASAS</li> <li>• ASD</li> <li>• ATCS</li> <li>• ATLAS</li> <li>• BCTP</li> <li>• BMC3</li> <li>• BSM</li> <li>• CINC CSA</li> <li>• CNCMS</li> <li>• CNPS</li> <li>• CR/HMS</li> <li>• CSCE</li> <li>• CSSCS</li> <li>• CTIS</li> <li>• C4IJM</li> <li>• DCARS</li> </ul>	<ul style="list-style-type: none"> <li>• DTSS</li> <li>• FATDS</li> <li>• FAAD C21</li> <li>• FIRESTORM</li> <li>• GCCS-A</li> <li>• GCSS-A</li> <li>• IBDAS</li> <li>• IMETS</li> <li>• ISYSCON</li> <li>• LW</li> <li>• MCCCC</li> <li>• MCS</li> <li>• MFC5</li> <li>• PEGEM</li> <li>• RCAS</li> <li>• SAS</li> <li>• TAIS</li> <li>• TCAIMS</li> <li>• THAADBMC3I</li> <li>• TPSOPS</li> <li>• TSIU</li> <li>• UAV</li> <li>• WARSIM</li> </ul>	<ul style="list-style-type: none"> <li>• AADC</li> <li>• CADRT</li> <li>• COMDAC</li> <li>• CCS</li> <li>• CUB</li> <li>• CV/TSC</li> <li>• GCCS-M</li> <li>• IUSS</li> <li>• JMPS UPCs</li> <li>• KSQ-1</li> <li>• LAMPS</li> <li>• MEDAL</li> <li>• METOC</li> <li>• MPA</li> <li>• MPAS</li> <li>• MSBL</li> <li>• NAVSSI</li> <li>• NFCS</li> <li>• NSPF</li> <li>• NSS</li> <li>• NSSN</li> <li>• PTW</li> <li>• REDS</li> <li>• SFMPL</li> <li>• SH60 MPS</li> <li>• SRMT</li> <li>• SCCS</li> <li>• TACLOGS</li> <li>• TAU</li> <li>• TEAMS</li> <li>• TERPES</li> <li>• TCAC</li> <li>• TDSS</li> <li>• TTWCS</li> <li>• VTC</li> </ul>	<ul style="list-style-type: none"> <li>• AF Weather</li> <li>• AMC BDM</li> <li>• AMS</li> <li>• AWACS</li> <li>• A2IPB</li> <li>• CSEL</li> <li>• DCAPE5</li> <li>• Defense IEMATS</li> <li>• FORTE</li> <li>• GBS</li> <li>• GCCS-AF AETC</li> <li>• GCCS-AF IF</li> <li>• IMDS</li> <li>• IMOM</li> <li>• ISC2S</li> <li>• MAMS</li> <li>• Rosetta</li> <li>• SBMCS</li> <li>• STRATCAT</li> <li>• TBMCS</li> <li>• AFDI</li> <li>• ARTDF</li> <li>• GALE</li> <li>• GCCS</li> <li>• GCCS-13</li> <li>• GCSS</li> <li>• JCACTD</li> <li>• JCALS</li> <li>• JDISS</li> <li>• JDP</li> <li>• JMC5ID</li> <li>• JMPS</li> <li>• JSCGS</li> <li>• JTAT</li> <li>• Joint Tactical Term</li> <li>• Joint Targeting Tool</li> <li>• JWARN</li> <li>• MEPED</li> <li>• MIDB</li> <li>• TNP</li> </ul>

Figure 5

Now let's see the DII COE at work (Figure 6). Several DOD systems, notably the Global Command and Control System and the Global Combat Support System (which we call GCCS and

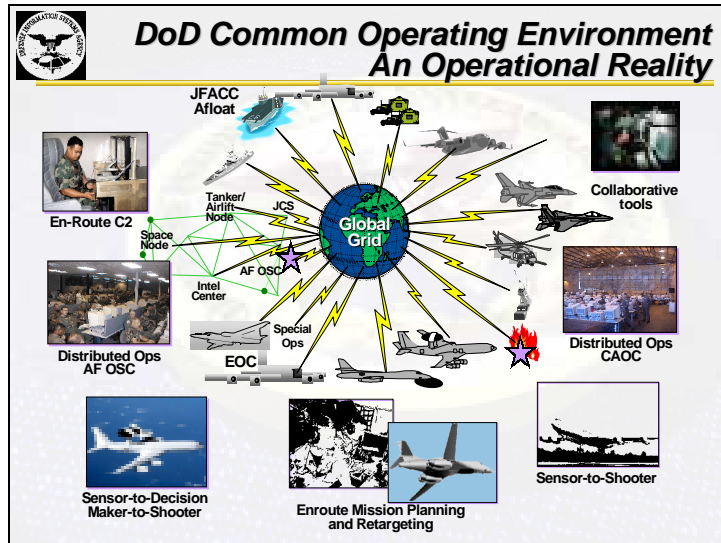
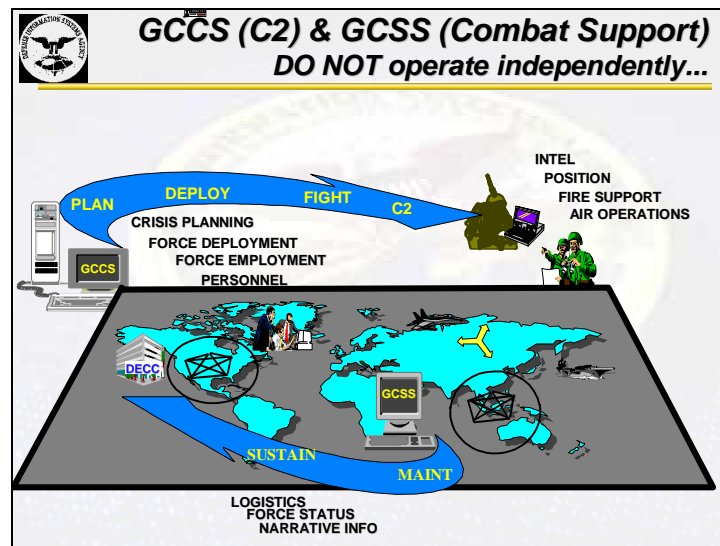


Figure 6

GCCS), and the Theater Battle Management Core System [TBMCS], are built on the DII COE infrastructure. As you saw on the previous slide [Fig. 5], many other systems are being planned for migration to the DII COE. These systems, linked through the GIG, will include sensor systems and weapon platforms, in addition to C2. With both sensors and weapon systems operating in a real-time arena, and with time-critical targeting becoming increasingly important, applying DII COE concepts to real-time C2 is a powerful method to enhance interoperability.

I mentioned that both GCCS and GCSS are built on the DII COE. This slide (**Figure 7**) shows, in broad terms, the relationship between these two systems. GCCS provides planning, deployment, and employment capabilities. GCCS is perhaps best known for its common operational picture (what we call the COP), which shows a “god’s eye” view of the battlespace—the air, land, sea, and space pictures, if you will. However, that is only a portion of its vast capability. By contrast, GCSS provides a wide variety of combat support capabilities and is the sustainment and maintenance system for the deployed force. GCCS and GCSS are two inseparable sides of a single coin. This slide shows how they come together to support the warfighter.



**Figure 7**

The next slide shows a great example of successful interoperability (**Figure 8**). GCCS is used at over 620 sites—many of them deployed—providing direct support to our expeditionary forces. From Bosnia to Kosovo to East Timor, GCCS has proved itself the preferred C2 tool.

Among the upcoming improvements to GCCS are, first, the Common Operational Picture-Combat Support Enhanced [COP-CSE], which enables a user to query and display logistical information on tracks, sites, and operations. Second is integrated intelligence, and imagery, or I3, which enhances situational awareness by overlaying imagery, order of battle, and target data on the GCCS COP. This is a big boost to the intelligence community. They really like this piece, and they pushed us in making this a great application for GCCS. Third is the GCSS portal, a Windows NT®-based, Web-enabled query tool that displays the same data as the COP-CSE, but in narrative format. Fourth, there's the COP-Transportation Support Enabled, which allows

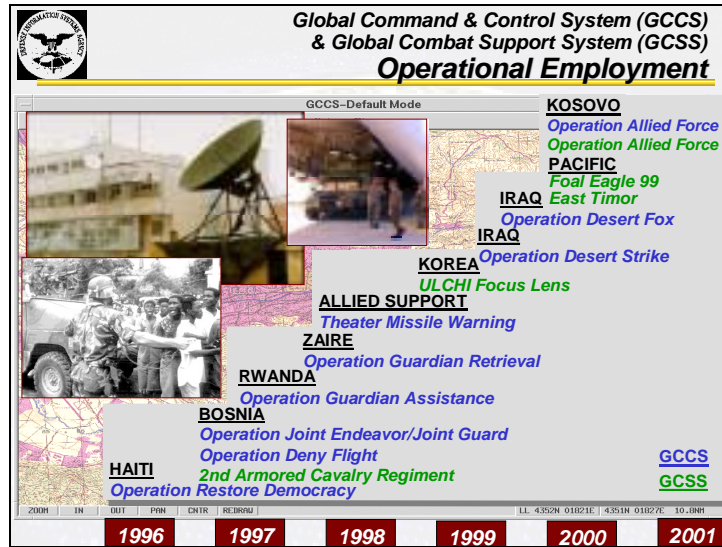


Figure 8

visibility over DOD transportation and supply assets. Fifth is the COP-Space Common Tactical Data, which provides predictions of vulnerabilities in satellite sensor coverage. Sixth and last is the Readiness Assessment System, which is a set of comprehensive query and reporting tools used to retrieve and analyze data from various databases.

Those are only six examples of things we're now building and streaming off the DII COE—that common C2 foundation, with common standards. When people want to bring applications that will help them perform their functional area of business better, they will build their applications based on that foundation. In the past, everybody built their own new systems, paying the same amount of money for the common standards, or the common foundation, over and over again. Contractors have benefited immeasurably from that. Now, we've already bought that common foundation—millions of lines of code that we have established as our standard—so we can get on with the specific, unique applications. This has been a tremendous benefit to all of us. Common interoperability comes from having that common foundation we can build on.

**Oettinger:** Let me be sure I understand. Are those standards for hardware, software, or both?

**Raduege:** They are standards for hardware that allow lots of different hardware pieces to be used as long as they meet a common standard, rather than mandating just one piece. It's not standardization; it's standards. It's not saying, "You can only buy a Dell computer," but it's requiring that a hardware platform meet a standard that's usually based on capacity, speed, and all that. If you buy a 386 computer these days, you are not going to be interoperable with the stuff we're going to throw at you. You are not going to be mainstream. You wouldn't buy a 386 or a 486 for your house these days, because you know you're not going to be able to do much on the Web.

We established common standards of hardware, but this then becomes a kind of standardization of software, because you have to use software that is compatible with those hardware standards. It's been built and it's been paid for once, and we only want to pay for it once, not multiple times. That's what we build our applications on.

**Student:** Is that Solaris based? UNIX?

**Raduege:** There's some UNIX, as you know, and then there are other systems. We're working some of this with legacy systems. There's a lot of UNIX, but we're also going away from UNIX-based systems in many cases. There are standards that we build on, and Solaris is one of them.

**Student:** When you talk about common code, is it classified or unclassified? Are people attacking it?

**Raduege:** It's not classified. It's actually based on commercial off-the-shelf [COTS] software that has been modified for our needs. The way we keep people from getting into that is through other means: through firewalls, guards, intrusion detection, and all that. We give this software away to our allies, because if we're ever going to have coalition interoperability we have to provide that to them. This is not based on a classified database or platform or foundation. It's COTS equipment that we bought and paid for, but we only wanted to do it once. Commonality not only allows us to have joint interoperability among Army, Navy, Air Force, and Marines, but it also begins to allow us to have coalition and allied interoperability.

**Student:** The East Timor operation jumped out as unique situation where the United States had minimal or even no direct combat support functions [Fig.8]. What specific things did we do to help the Australians in their operations? Is there anything you can tell us about that?

**Raduege:** Oh, boy! The real pace-setter there, and the difference, was that this was a commitment by the U.S. government, probably for the first time since World War II, of U.S. forces working for an allied government. The Australians were in charge of the operation. We provided support. It's interesting, because we didn't employ the C2 system (GCCS); what we employed was the combat support system (GCSS), which is logistics and those kinds of things. I'm not an expert on the East Timor operation, but it was more along the lines of providing assistance to the Australian-led force structure with a combat support system, with U.S. forces being employed in the process.

**Student:** Staying with the theme of interoperability, I read a great deal about the Navy-Marine Corps Intranet [NMCI]. Does that incorporate this commonality of code and hardware? Even though the Navy and Marine Corps are traditionally lumped together, are the other services still building up their intranets? Is there still a disconnect in commonality?

**Raduege:** At about the time I got to DISA, the Navy was going to contract on NMCI. There are some instructions in the DOD that say that if you're going to build any type of network and it's not going to be with DISA, you have to have a waiver. As you saw on that first chart I showed you, with DISA's history [Fig. 1], in the 1960s each service used to buy its own communications equipment. Then we ended up with problems like those in Grenada, where we weren't interoperable. That's why an organization like mine was created: instead of having each individual service buy its own communications, you have one organization that buys for all and gets the benefit of reduced cost, because it buys in bulk.

The NMCI was going against that philosophy, and the DOD would not issue them a waiver to the policy for putting their systems under DISA. We entered into serious negotiations with the Office of the Secretary of Defense [OSD] and the Navy on the issue of using the joint enterprise network. Both OSD and the Navy signed up to that as part of a memorandum of agreement.

When the contract was then let, the Navy was going to end up paying for long-haul communications through their contractor, because it was part of the seat cost,<sup>5</sup> and they were also going to end up paying DISA to provide them with the same long-haul communications, because that's part of the way the DOD does business. The Navy and Marine Corps found themselves in a dilemma. They either had to modify the contract or pay for communications twice. This is still an ongoing issue. We, of course, believe they should modify their contract and live up to the agreement they signed with the OSD and with us.

What do we do to solve that problem? Part of being on the DISN [Defense Information Services Network], the DOD's communications network, is that you get joint interoperability and assured security. I will tell you today that one of the CINCs asked me, "Harry, when the Navy and Marine Corps come to my theater of operations and we have to put together a JTF or some sort of joint operation, will the Navy and Marine Corps be able to communicate with the Army and the Air Force and the other agencies?" I said, "I'm not sure what's in the contract to allow that, because I'm not sure of the interoperability specifications you asked for or the security aspects. But if they are on the DISN, I can assure you of interoperability and I can assure you of security." This is a big deal to a CINC, and one of the key issues here is the CINCs' viewpoint versus the military services' viewpoints.

I am not going to argue this out in the media. We have promised ourselves that we're going to work it out at the negotiating table among the Navy, Marine Corps, DISA, and the contractor involved, rather than arguing one another or putting things into the news. That's exactly what we're going through right now.

Remember that I just mentioned six things we were doing with GCCS? They found no fewer than 4,000 different applications in Navy Air that weren't on the contract; they were additional to what the contract called for. What to do? You've got to address that. I work with the Navy chief information officer, Dan Porter, on these things. We're having program reviews to make sure we're working together on all this. We're talking about lots of issues that have to be worked out, and that's just for the continental United States [CONUS] piece, because this also has to go globally. That may mean different contracts have to be let, because this was not a global contract. How do you ensure interoperability if you're going to have different contractors getting different pieces of the overall NMCI?

**Oettinger:** At the risk of belaboring the obvious, may I state a footnote and see if you agree? By the time he's gotten this problem solved, two things will have happened. One is that the fundamental structural problem will remain, and the second is that the technology will have changed radically, so the architecture will have to change and the whole process is continually iterated. I want to underscore a point that I keep making with you: this is a dynamic process. There are no answers that stay put for more than five minutes. If you don't carry anything else away from this course, that is an essential point. You've had it illustrated here about as forcefully and concretely as one can imagine. This is the norm. It is not anomalous. You're not looking at anything unusual, and I don't see it going away, unless the Constitution of the United States is changed or there is a total moratorium on research and development in technology.

---

<sup>5</sup>The seat cost is the annual cost of installing and sustaining a suite of computing tools for an individual user or client within a network and training and equipping the user or client.

**Student:** This is an editorial comment, sir, and you may agree or disagree. One thing that has changed significantly is that you have a DISA organization that has credibility way beyond anything it's ever had in the past. With that organization capable of doing what it does today, when these decisions have to be looked at again tomorrow, and other organizations have to decide whether to come on board or go it alone, I think the decisionmaking process is going to be considerably different and the ability to move forward quickly and stay interoperable is going to be made easier because of the improved perception of your agency.

**Raduege:** I appreciate that. That's exactly why I added that customer focus to our equation.

I want to foot stomp what Tony has said. In life, and in your business (because many of you are out there at midpoints in your careers), when you're in a management position, there are often no exact black-or-white answers to things. The skills that you're developing at these kinds of schools help you manage the chaos out there. They help you remain calm and not go ballistic over everything, or you'll end up in the hospital and you'll be no good to anybody. No amount of education and long-term development is going to help if you end up going ballistic over everything that you can't make "right," or to your liking. So you've got to work with people, and you've got to work with all the different pieces of the equation, and that example I just gave you shows you how complex these things can be.

We're trying to address these issues professionally, to keep calm, work it out, and not let the media create a circus, because they can have a lot of fun with this, pitting generals and admirals and senior civilians against one another. I won't take that, and nobody at my organization will stand for it either.

There are a lot of things that are like that: highly complicated. This is a \$7 billion initiative. That's a lot of money. People will do many things for \$7 billion...or not do things. They don't move.

It's part of my daily life. You have to manage this chaos. You're in the middle of it all the time, but the skills you're learning here are going to help with that.

Getting back to GCCS, deployed commanders use GCCS not only for situational awareness but also for deployment and redeployment planning. We track and provide status on millions of objects. We push information forward—sometimes over low bandwidth and unreliable communications—based on warfighter requests.

DISA's GCSS efforts are focused on supporting the unified commanders by providing a fused and integrated combat support picture to commanders at the CINC and JTF levels. This capability will be fielded as a GCCS mission application to provide commanders with read-only access to combat support information in the GCCS operational environment. Together, GCCS and GCSS provide a total integrated battlespace picture incorporating both C2 and combat support information. From the key at the bottom of the slide [Fig. 8] you see that we started this in 1996, so some of the folks who spoke here before probably talked about the GCCS.<sup>6</sup>

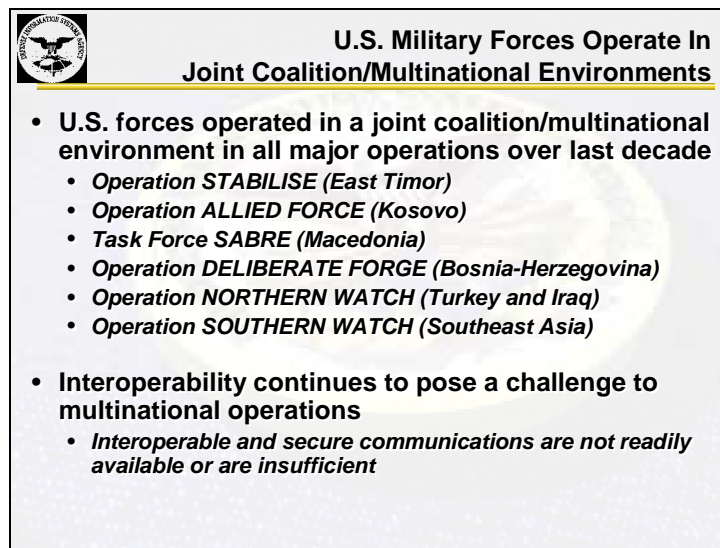
---


<sup>6</sup>For earlier discussions of GCCS, see the following in various volumes of the *Seminar on Intelligence, Command, and Control* (Cambridge, Mass.: Harvard University Program on Information Resources Policy): David J. Kelley, "Providing Global Information Services to the Warfighter," in *Guest Presentations, Spring 1999* (I-00-2, June 2000); and Albert J. Edmonds, "Information Systems Support to DOD and Beyond," in *Guest Presentations, Spring 1996* (I-97-1, January 1996); "Integrated Information Systems for the Warrior," in *Guest Presentations, Spring 1996* (I-96-2, January 1997); and "C4I Issues," in *Guest Presentations, Spring 1994* (I-95-3, January 1995). All available at URL:

Last month [March 2001] we received approval to begin fielding GCSS to Pacific Command [PACOM], Central Command [CENTCOM], and Joint Forces Command. We expect to receive approval this summer to proceed with global fielding of GCSS to all unified commands by the end of this year. So, just like GCCS, GCSS—the combat support element that complements it—is coming on line in this time frame. These are tremendous success stories of how you work an interoperable system across the entire DOD and convince everybody that buying into it is the right thing to do, even though they can spend their money any way they want because military services can do that.

We are getting better at the information interoperability game (**Figure 9**). The DII COE, GCCS, and GCSS are only a few initiatives in this area. I believe it's better to solve interoperability problems now rather than on the fly while deployed to a remote mountaintop or in harm's way.

Today's world has changed. Our U.S. military forces must continue to be jointly interoperable, but they must also be able to communicate with the forces of other nations. Every operation we've been involved in over the last ten years operated in a joint, coalition, or multinational environment. Nonetheless, coalition interoperability continues to pose large challenges to our deployed forces.



 **U.S. Military Forces Operate In Joint Coalition/Multinational Environments**

- **U.S. forces operated in a joint coalition/multinational environment in all major operations over last decade**
  - *Operation STABILISE (East Timor)*
  - *Operation ALLIED FORCE (Kosovo)*
  - *Task Force SABRE (Macedonia)*
  - *Operation DELIBERATE FORGE (Bosnia-Herzegovina)*
  - *Operation NORTHERN WATCH (Turkey and Iraq)*
  - *Operation SOUTHERN WATCH (Southeast Asia)*
- **Interoperability continues to pose a challenge to multinational operations**
  - *Interoperable and secure communications are not readily available or are insufficient*

**Figure 9**

At the risk of being parochial, let me tell you that this little stool here has helped me in many sessions over the past five or six years (**Figure 10**), because when you work in a highly technical environment somebody always wants you to describe the problem in twenty-five words or less. I deal with high-level officials, and they don't want some bit-bucket type of explanation. This is something that I can always draw on. I've used it countless times, and I want to share it with you. Joe [Joseph E.] Hurd, a very smart fellow who was J-3 in CENTCOM and over in

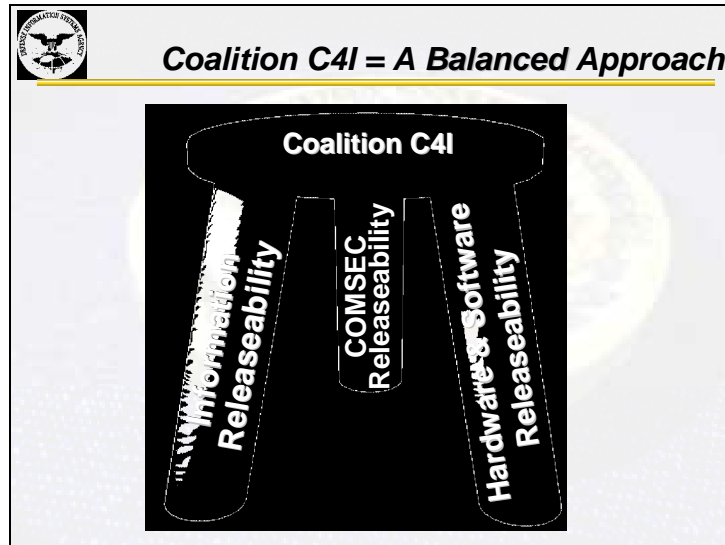


Figure 10

Korea, and retired as a three-star general, described coalition C4I in this fashion, because he was from a farm in Kentucky. Coalition C4I is one key enabler that IT provides, but that is not a simple task. It requires an entire infrastructure, organization, and components to collect, process, store, transmit, display, and disseminate information. A simple device like this three-legged stool can be useful to illustrate the point.

Some areas of responsibility, such as Europe, have organized structures, such as the North Atlantic Treaty Organization [NATO], that aid coalition interoperability efforts. Other regions, such as the Pacific, lack such structures, thus adding additional challenges to our coalition interoperability quest.

Take the leftmost leg, “information releasability.” For us, information sharing must follow the U.S. International Traffic in Arms Regulation and must be consistent with the Arms Export Control Act. Specific information releasability is determined by the Combined Interoperability Working Group, our Joint Staff, the unified CINCs, and the U.S. State Department. These organizations also work the associated restrictions on exporting encryption.

**Oettinger:** How many lawyers do you have on your staff?

**Raduege:** I think I have five or six, and I work them very hard.

**Oettinger:** Again, there’s a tendency to joke about this or to regard it as a perversion, and I think it’s wrong. You’re dealing with fundamental structures of U.S. checks and balances, and if you don’t have lawyers on your staff you’ll screw this up. So ignore the jokes about lawyers; they are an essential part of your staff.

**Student:** Nicholas Rostow said the same thing when he was here a few weeks ago.<sup>7</sup>

**Raduege:** Absolutely. I don’t even tell lawyer jokes anymore. The decisions I have to make that are very important I run by the attorneys, and they always find something that I could get into

<sup>7</sup>Nicholas Rostow spoke at the seminar on March 15, 2001.



trouble over or could obligate the U.S. government in a bad way. So praise your attorneys! They are good folks. They do good work for us. I think the reason the lawyer jokes come about is that we know how good they are and we appreciate them so much and sometimes they have to take the brunt of that unconditional “love.”

**Student:** Tough love!

**Raduege:** Next, let’s look at the rightmost stool leg, “hardware and software releasability.” For software, source code changes may be required for release, while for communications security—the center “COMSEC” leg of the stool—releasability requires appropriately approved equipment, which is often in short supply. However, the good news is that the Joint Staff, the National Security Agency [NSA], and the National Security Telecommunications and Information Systems Security Committee have an effective process in place for releasing COMSEC equipment among our coalition partners. General Mike Hayden, the NSA chief, spoke at your seminar last week, and COMSEC releasability is his responsibility.

The rightmost leg means foreign military sales, on a case-by-case basis, involving the State Department. Information releasability, on the left, involves the Joint Staff as to which information we can release to which ally or coalition partner, and that is a matrix. One shoe doesn’t fit all in these cases, so this is very complex.

That’s the little milking stool, and if you don’t have all three of those legs, the stool falls over. If you have information releasability and COMSEC and you don’t have hardware and software releasability, you don’t have coalition C4I interoperability.

Through a series of operations and exercises, some of which are listed on this slide (**Figure 11**), we work closely with the CINCs to improve combined and joint interoperability. Through these missions, we also enhance security relations and demonstrate U.S. resolve to support the

The slide features the Department of Defense seal in the top left corner. The title "Coalition Interoperability" is centered at the top. Below the title is a bulleted list of exercises and programs. To the right of the list is a photograph of a military vehicle in a field, with the caption "East Timor, Operation STABILISE" below it. At the bottom of the slide is a horizontal strip of small, square images showing various military personnel and equipment.

- **Exercises and Operation Successes**
  - Operation Stabilise
  - Cobra Gold
  - Operation ALLIED FORCE
  - Combined Endeavor
- **Asian Pacific Network (APAN)**
- **Coalition WAN**
- **USCINCPAC's Command & Control Interoperability Program (CIP)**
- **Joint Interoperability Test Command Interoperability Guide**

Figure 11

security and humanitarian interests of regional friends and allies. Another ongoing initiative is the Asia-Pacific Area Network, known as APAN, a Web-based network designed to link the nations of the Asia-Pacific region. APAN's mission is to communicate and share information electronically to facilitate regional understanding, promote confidence among Asia-Pacific neighbors, and enhance security cooperation. APAN is a tool to get "the right information to the right person at the right time to make the right decision." If that sounds familiar, it's because that's what Admiral Blair said, as I quoted earlier, and the Pacific is his area of responsibility.

The DISA Joint Interoperability Test Command at Fort Huachuca, Arizona, is working another key issue for multinational operations: an interoperability guide that gives planners an interactive tool showing which systems interface within the region, whether they be radios, switches, routers, or multiplexers. This guide is based on experience gained in Europe's Combined Endeavor 2000, the sixth in a series of U.S. European Command-sponsored exercises designed to identify, test, and document communications and information systems interoperability between NATO and the military equipment of the "Partnership for Peace" nations. CINCPAC's Command and Control Interoperability Program could provide a basis for this effort as the seven participating nations work through interoperability issues and gather the necessary data. This effort could, in turn, be expanded to include others of the forty-four focus nations in the region.

**Oettinger:** Before you leave that slide, in case some of you civilians wonder what that has to do with the private sector, just think of it not as coalition interoperability but as business to business. You have exactly the same problem, so this is a very general set of issues.

**Raduege:** Another way to achieve interoperability is to purchase the DII COE—that approved and releasable system I talked about earlier (**Figure 12**). DISA offers a variety of products and services to the U.S. armed forces, our allies, and coalition partners. We deliver integrated and interoperable C4 systems and the infrastructure to maintain these services and systems. We also

The slide features the Department of Defense seal in the top left corner. The title "Foreign Military Sales" is centered at the top in a bold, italicized font. Below the title is a bulleted list of services: "Integrated C4I Systems" (with sub-points for GCCS and GIGCOE), "Infrastructure Systems/Services" (with sub-point for DISN), "Engineering Services" (with sub-points for Site Surveys, Architectural Studies, and Contract Services), "Information Security", and "C4I Integration Services". To the right of the text are four small images: a person in a white shirt, a person in a red hard hat, a person in a white shirt, and a tall antenna tower.

Figure 12

provide engineering, information assurance, and C4I integration services. These products and services are worked on a nation-by-nation basis, as eligible, under the Foreign Military Sales program. We're not just saying, "We've got it, and you can't have it."

**Student:** General, even though you offer these products and services for foreign military sale, do you find reluctance among some of our allies for the same reasons that they're reluctant to buy other U.S. hardware systems: because of their own infrastructure, suspicion of the United States, et cetera?

**Raduege:** Absolutely. They're reluctant for all of those reasons, because, let's face it, everybody wants to compete in the global markets. They want to sell their equipment or create jobs for their people and not just buy from us. This is part of that tug and pull. There's also the reluctance of, "Okay, if we buy something from DISA, is it going to have some sort of device in it that will eavesdrop on us?" All these fears have built up over the years. They are all part of the equation. This is not an easy process, like going out and saying "Here, buy us," and everybody saying, "Oh, great, let's do that." All sorts of political and other organizational issues come as part of the package that you have to work. Some people end up choosing not to be interoperable, just because it's not in their best interest at that particular time.

**Oettinger:** I can't overemphasize the permanence of that. If you look at the record of the seminar, and discussions of NATO interoperability, et cetera, that theme always recurs.<sup>8</sup> The reason things may have changed somewhat is that the Goldwater-Nichols Act [GNA] has shifted some muscle toward the CINCs (and whenever Harry refers to the customers I think he has the CINCs in mind), so that has changed, but the international dimensions have not changed at all. The constraints are not much different from what they were, except the GNA and the technology have changed, so he's solving the same problems all over again that his predecessors have wrestled with.

**Student:** What are the fallbacks if we end up working in a coalition with someone who has refused to buy the systems you're offering? Is that in your province?

**Raduege:** Usually, what we try to do is work out an agreement nation to nation. If they prefer another solution, and if it's somehow interoperable and isn't going to cause a problem for us or will allow the interoperability, we usually agree to that. We don't want something that will mess up our entire network or put vulnerabilities into it through a hardware or software device we're not sure of. It's our prerogative to say no. But we usually try to work these things out. We're not totally hard core.

**Student:** Has this program been successful in any particular CINCDoms, such as Central Command, for example?

**Raduege:** Very. First, let's just take GCCS. I spent three years at CENTCOM, and I worked that back in 1995. As a matter of fact, CENTCOM was the first one to take GCCS over into Saudi Arabia and Bahrain. The State Department has authority over the foreign military sale for the

---

<sup>8</sup>See, for example, Kelley, in *Guest Presentations, Spring 1999*; and Barry M. Horowitz, "The Emergence of Data Systems: Cost and Technical Change in Military Systems," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1993* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-94-5, August 1994), [On-line]. URL: <http://www.pirp.harvard.edu/pubs.html>

hardware and software of GCCS. They gave that responsibility to the assistant secretary of defense for command, control, computers, and intelligence [ASD C3I], who in turn gave it to DISA. We ended up being the organization that provided one leg of the stool: hardware and software; in other words, GCCS terminals and GCCS software. For information releasability we worked with the Joint Staff to find out what we could tell the Bahrainis, the Saudis, the French, the Brits, or whoever came to the table in an operation we were working over there. As I said, that's a matrix. Those are things that take place nation to nation. We were able to work out what we could give people for that leg of the stool.

The most difficult part was the COMSEC release. I had the other things in place, but then I had to work the COMSEC piece through the NSA. We had to have a memorandum of understanding between the United States and each one of those nations. They were bilateral agreements; we can't just have one agreement for everybody. The people responsible for it in the United States want to sit across the table from their foreign counterparts and talk about how they will protect this COMSEC, because when you give it to somebody it has to be protected in a certain fashion.

**Student:** You're giving them the same codes we use?

**Raduege:** Yes, but we don't give anyone our TOP SECRET stuff. We don't give anybody the kind of thing that was on the EP-3.<sup>9</sup> That is United States only; no exceptions. There are other releasable elements that are very good. We rely a lot on the Internet with PKI [public key infrastructure] encryption that's very good. You trust all your credit card information to it, because you're probably out there ordering stuff all the time. That's pretty good encryption, but that's commercial encryption. The NSA releasable encryption is higher than that, so the nations that signed up to that, with whom we have agreements, are getting a very good deal for national security. It's still not as good as our best, because we won't sell our national treasures. We won't take a chance. There are different elements of what we release, and we work those memoranda at the releasable NSA COMSEC level. Everybody can sign up to get PKI stuff, because that's a commercial product. How safe do you feel?

**Student:** Pretty safe.

**Oettinger:** After all, your liability is limited to \$50 or so.

**Raduege:** Sure. It's not your life, or your son's or your daughter's life. We won't give that away.

**Student:** Sir, how involved is your agency in the negotiations about declaration of principles with our major allies for increasing interoperability of our industries? How involved is DISA in general in industry-to-industry interoperability and cooperation with our allies to ensure that there's interoperability of our systems at the ground level?

**Raduege:** First, let's talk about allies. I'm getting ready to go over to London next month for a meeting of the Combined Communications-Electronics Board [CCEB], where I will give a speech to some of our closest allies there: the Brits, the New Zealanders, and the Australians. We actually set up the CCEB years ago. It's got some old terminology in it: comm-electronics is an old term, but we keep it because everybody knows what the CCEB is. We meet with our allies and we discuss common areas of interoperability and work through these issues.

---

<sup>9</sup>A reference to the plane forced down in Chinese territory on March 31, 2001.

Over a number of years, we also set up something called a coalition WAN [wide area network], and we have computers and communications set up on those links. We share that WAN and work through interoperability problems on that all the time. Every year we put new applications on the WAN and try them out to make sure they will interoperate and will provide our closest allies with the newest capabilities.

In my previous command I was at North American Aerospace Defense Command, and I worked with the Canadians. We've got binational agreements with Canada, and we exchange a lot of information at the top level.

It's interesting you should mention industry. In my other hat as the head of the NCS, one of my responsibilities is to be the designated federal official for something called the NSTAC: that's the National Security Telecommunications Advisory Committee. It is an advisory council that has been around now for eighteen years. The president of the United States, through executive order, has allowed me to recommend thirty of the top chief executive officers [CEOs] in the IT business to sit on it. I've got one chair open right now, and I have lots of candidates. Dell wants a seat; Compaq wants a seat; AOL wants a seat. Tony mentioned you had the banking industry here not too long ago,<sup>10</sup> and I was wondering if it was Donald Obert of the Bank of America, who has set up a banking industry ISAC—what they call an Information Sharing and Analysis Center.

I think you will recognize the NSTAC principals I have: AT&T, Bank of America, BellSouth, Boeing, Cisco, Computer Sciences Corporation, EDS, ESET [Executive Security and Engineering Technologies], ITT, Hughes, Lockheed Martin, Lucent, MCI WorldCom, Microsoft, Motorola, Nortel, Northrop Grumman, Qwest, Raytheon, Rockwell International, Science Applications International, Sprint, TRW, Teledesic, U.S. Telecom Association, Unisys, and Verizon. I have to decide which one of those others I mentioned to you to recommend for that chair. Because this business involves hardware, software, security, and networks, I try to get people so that I have someone in each one of those disciplines.

NSTAC does not end up being a marketing scheme for these folks, because these are CEOs. It is a council where we talk about issues that are of national security and emergency preparedness concern to the United States of America. These CEOs come to me and say, "Harry, when we're sitting across the table from our competitors in that forum, we're not going to mention what our weaknesses and vulnerabilities are" (because they all have them and know they have them), "but we will tell you privately because of your responsibility as the manager of the NCS." When it's national security and emergency preparedness—when a tornado or a hurricane takes out a whole sector of the United States or rolls over some very important assets—you've got to get those kinds of folks together quickly to address the communications demands.

I happened to handle Hurricane Andrew when it rolled over Homestead Air Force Base in 1992. I'm going to do the David Letterman thing with you and ask you what you think the survivors' top three priorities were. They had come out of their houses and maybe found just a little piece of them left, or they had just had the eye of a hurricane run right over the top of their base. One person was in a hangar where the doors were blown off and an F-16 was blown through them. That's the force of this kind of disaster. We couldn't get the FEMA [Federal

---

<sup>10</sup>The speaker was actually Kawika Daguio of the American Bankers Association. See "Protecting the Financial and Payment System by Dispelling Myths," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1999* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-00-2, June 2000), [On-line]. URL: <http://www.pirp.harvard.edu/pubs.html>

Emergency Management Agency] down there fast enough. We put combat communications in there from Patrick Air Force Base to establish initial communications. The FEMA came out a while later. What do you think the number 3 priority was?

**Student:** Food.

**Raduege:** What do you think the number 2 priority was?

**Student:** Water.

**Raduege:** What was the number 1 priority?

**Student:** Communications.

**Raduege:** Communications. They wanted to call their loved ones and let them know they were okay, or, if they were outside the area, they wanted to call into the area to find out how people were. These are things that we normally just take for granted until we don't have them. When you look at the global perspective of humanitarian operations, disaster relief—some of the things I mentioned and showed on those earlier charts—when people are in those kinds of situations, they want communications. They want to be able to tell someone, “I'm okay,” or “I'm hurting,” or “Send help,” or “Do something.” Water was the second priority, and their stomachs started growling after a while so they wanted food. But we can go without food for a long time, especially after a disaster like that. I learned an interesting lesson, and it was really driven home by the disaster from Hurricane Andrew.

To get back to your question, the NSTAC allows me to meet with these CEOs, and on June 5–6 we're going to meet with the president of the United States, the vice president, the national security advisor, and the secretary of state. We're going to talk about issues of national security and emergency preparedness interest across the IT domain.

**Oettinger:** Let me give you a note on speakers of historical interest and the unintended consequences of policy decisions in different realms. NSTAC was created while Lieutenant General William J. Hilsman, one of General Raduege's predecessors, held the office. It was created to fill a void when the Department of Justice wanted to take AT&T apart, which the DOD fought for a long time. The DOD argued that this would take apart the one place where all these issues of national security and telecommunications were taken care of, and AT&T of course argued along with the DOD that they shouldn't be taken apart, because the United States would collapse as a consequence.

For over twenty years, we've had this kind of mechanism where multiple parties, rather than a monolith, are drawn together, and it works, but not without some difficulty. The guys sitting around the table won't admit to errors and flaws and vulnerabilities, but only whisper them to you. In AT&T, this was Bob Gradle talking to himself. It took one phone call from Lee Paschall<sup>11</sup> to one guy at AT&T—and he could identify him in those days—to straighten all of these issues out. By the way, it never got into anyone's budget, because AT&T buried the cost of aiding the DOD in the rate base and it amounted to pennies on your bill and mine. Once the civilian antitrust issue took AT&T apart, all these mechanisms had to be put in place to take care

---

<sup>11</sup>Lt. Gen. Lee M. Paschall was the director of the DCA (DISA's predecessor) and manager of the NCS from 1974 to 1978.

of a consequence that no one in the Justice Department had ever even thought of. So you get strange ways in strange realms out of decisions in one way or the other.

**Raduege:** Networking is about having these kinds of relationships you can call upon. These are people I work with, and know, and they've said, "We will tell you our company's secrets. We request, respectfully, that you don't reveal them to our competitors, but in the interest of national security and emergency preparedness we will tell you, because we're more interested in those things than in the dollar." That shows tremendous respect, and that's the CEO—the one who can make the decision for the corporation. That's why we work at the CEO level, but that's also why we're at the president's level, because those are pretty close.

To answer your question, that's how we work a lot of big industry-to-industry problems. Right now, we're working one issue of what we call the "last mile" of communications, because a lot of times you can get big pipes to a certain place, but then the problem becomes dealing with the local place to get it in fast, because you can't wait six months for somebody to process the paperwork and all that kind of stuff. You've got to get on with business. We're working the interoperability for national security and emergency preparedness at the CEO level, and we're talking to the president about it.

**Oettinger:** For the civilian counterpart to that, look at the book by Reed Hundt, the former chairman of the Federal Communications Commission, on the parallel problem of going the last mile for schools.<sup>12</sup> It happened on his watch, and it involved the president and the vice president to get some of that done. The parallels are there. It's amazing how these things require high authority.

**Student:** How much do you work with international business, in which the DOD lets contracts to make sure there's interoperability there, especially regarding coalition forces? I just completed a big report for the DOD Office of Industrial Affairs. They really wanted to look at international mergers and acquisitions, because we now have Nokia, Ericsson, and all these Dutch firms that are DOD contractors.

**Raduege:** International organizations—and even our own organizations, which may be foreign owned (that's happening a lot more these days)—tend to market products based on uniqueness. You just don't make the same products somebody else does and carve out your place in the economy unless you make it better and cheaper. Then you might have a chance. Most people try to create and sell products based on a unique quality, and then everybody's got to have it. That's how they sell.

In our business, this uniqueness creates the problems and the wedge in interoperability, because by creating something that's a unique service, you're driving the market away from commonality, standardization, or something that's based on a standard, because it's new technology. We constantly have that problem of trying to be on the leading edge of technology, but not on the bleeding edge. It's a total balance issue.

I went out to the West Coast a couple of weeks ago and visited eight big companies: Cisco, Hewlett-Packard, IBM, Microsoft, Global Crossings, those kinds of places. I talked to them at the senior vice president level, and each of them spent a half day with my team. Part of what we tried

---

<sup>12</sup>Reed E. Hundt, *You Say You Want a Revolution: A Story of Information Age Politics* (New Haven, Conn.: Yale University Press, 2000).

to drive home to them was, “We need you to build systems and networks, software and hardware capabilities, that will allow for interoperability and commonalities. We need to have standards that allow us to buy from multiple vendors.” That rubs against them sometimes. They really don’t want to hear that, because they like the battle. They like to say, “It’s either *this* or *this*. You choose.” They want to sell you their product.

When most of us have to choose between a Macintosh and an IBM PC, or a Betamax video recorder versus VHS, we usually wait to see who’s going to win. Some of us have Betamax tapes up in the attic, and guess what? Technologically they were better, and they’re still known to be better. As a matter of fact, a lot of news media today use beta to record on, and then they translate the recording into VHS, but Betamax is higher quality. Most people also recognize that Macintosh computers are much more user friendly than IBM PCs, but who won the marketplace? What are you going to bet your business on?

Yesterday Craig Mundie, who is the senior vice president of Microsoft, briefed my committee of principals on what he sees as the future of the Internet, where it’s going, and what the vulnerabilities are going to be. That committee is the federal arm of my NCS hat; its members are FEMA, State Department, Commerce, Interior, the White House, the General Services Administration, the Federal Aviation Administration, and some other civilian agencies. When I met with him in Seattle, he said, “You know, Harry, the DOD is Microsoft’s biggest client, but you still represent less than 1 percent of our business.” They like to listen to us, but 99 percent of their business is spread across all other kinds of folks. We’ve all migrated toward that.

I can remember being at Langley Air Force Base in 1992 and trying to choose *the* e-mail system for Air Combat Command, which was the largest command of the entire U.S. Air Force. That system was going to populate a lot of places, so think about that for interoperability! We set up a testbed area, and we brought people from the staff out there and let them try all the available e-mail services, and there was a whole bunch of them. The technical folks liked one called Beyond Mail.® Beyond Mail had all kinds of neat features, allowing you to sort and parse. You could put a word in, and *zip!* you’d have a sorted list. You could do that if you wanted to search a document or a series of documents. That was pretty high-speed at that time. It’s antique to us now, because we do that stuff all the time. It was something Microsoft didn’t provide. Of the ten or so systems we checked out, my engineers voted for Beyond Mail, and it got 40 percent of the votes. Other people liked Microsoft, and it also got 40 percent of the votes.

The guy I worked for at the time asked, “Harry, what do you think we should do?” and I said, “I don’t know; this Microsoft Corporation seems to be on the move. It looks like the power base may be there in the future. I’d go with Microsoft.” We went back to the office, and he called the Microsoft folks. They were right there (as they may be today) with customer service—front-line support. “What can we help you with?” “We just did a fly-off over here, and we were looking at different e-mail capabilities. The engineers really liked the capabilities of Beyond Mail, but we also liked yours. Can you accommodate that in any way?” The representative said, “Let me check, and I’ll call you right back.” (By the way, she was not quite one of the original fourteen, but she was really close behind that. She’s already got her millions and billions. She may be out fishing today.) She came back about three days later, and said, “We’ve got the problem solved. We can do that for you.” My boss asked, “How are you going to do that? Did you develop that capability already?” “No, we just bought it.” They bought the rights. They bought the ma-and-pa operation, which was a small company. Don’t feel sorry for ma and pa,



because they're in early retirement city right now. They probably went out and invented something else that Microsoft bought later on.

There's something to be said about that kind of power. Like it or not, you can go with the other one and maybe end up being a loser. You've got to be careful with these kinds of things, and you've got to work with people.

**Oettinger:** If and when the Justice Department breaks up Microsoft, you'll be in the same situation. You'll need to expand the NSTAC mechanism to include the whole software area as well as the telecommunications area.

**Raduege:** It's tough. As I said, right now I have Dell, Compaq, AOL–Time Warner, and one other who want my one available seat, and I have to make a recommendation on that.

**Oettinger:** There's another footnote on that. It started out as the National Security *Telecommunications* Advisory Committee, and see how stretched that definition has become? AOL–Time Warner? Cisco? Those guys didn't exist even in people's imaginations when NSTAC was created.

**Raduege:** We've often had those thirty seats occupied, and all of a sudden a seat becomes available. Why does that happen? Because there are mergers. One member company buys another. It has happened many times with the companies sitting at the table right now, and that's just part of the operation. It happens all the time.

We work with industry and we work with allies, but when we're working with international providers, we also really have to work with our providers. In my conversations with Cisco, I don't have a lot of leverage because I'm with the DOD. I've got to go on what the marketplace provides. I'm not a driver of the marketplace. The DOD used to be, but those days are gone. Nobody jumps for the DOD anymore. That's why we had to go to common standards and COTS equipment: we don't have the amount of money to develop our own stuff as we used to back in the good old days, if you will. Maybe they weren't such good old days, when you think about it, because we used to have long periods of time to acquire things, and in IT, if you're talking long periods of time now, you're just buying a bunch of old garbage and living with it.

**Oettinger:** That's a wonderful introduction. If you want to go into much more depth on this whole standardization issue, there's a book by Martin Libicki on standards.<sup>13</sup> He used to be at the National Defense University; he's now at RAND, and he's writing on all this.

**Raduege:** During Noble Anvil, which was Kosovo, a total of 855 megabits per second were provisioned, including 1024 circuit actions (**Figure 13**). DISA-Europe worked closely with the CINC and the services to ensure timely and accurate communications employment. This yielded significant increases for the southern region, as well as increases for intertheater links from Europe to the continental United States, some of which carried time-sensitive Predator—surveillance—video. You can see that this was a tremendous buildup of capability. They started with about 200 megabits, and now there are 855.

---

<sup>13</sup>Martin C. Libicki, *Information Technology Standards: Quest for the Common Byte* (Boston, Oxford, Melbourne, Singapore, Toronto, Munich, New Delhi, Tokyo: Digital Press, 1995).

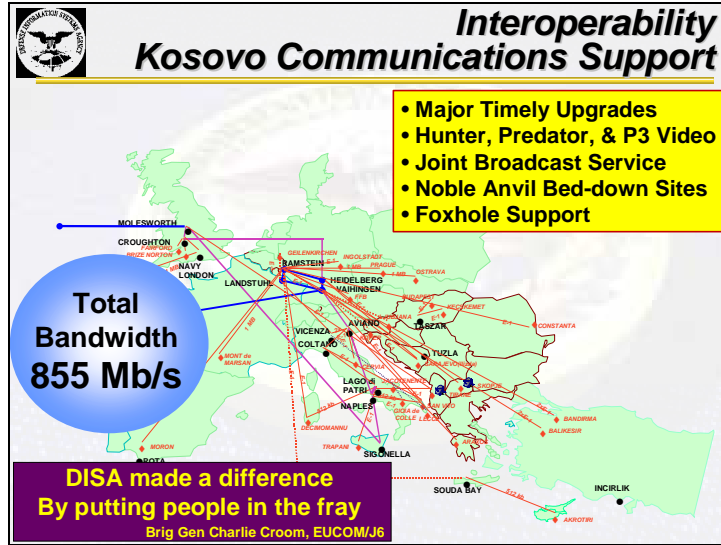


Figure 13

Remember the milking stool? We just modified it. Because of today’s large requirement for information, we’ve added one more leg to our coalition stool, making information an even stronger “coalition C4I chair” (Figure 14). Our new leg, bandwidth, promotes the flow of information throughout our coalition partners. We recognized that if we were no longer restricted by small communications connections, we could find ways to exchange voice, imagery, data, and graphical information at near-real time. The goal is to increase information throughput incrementally, based on the situation at the time.

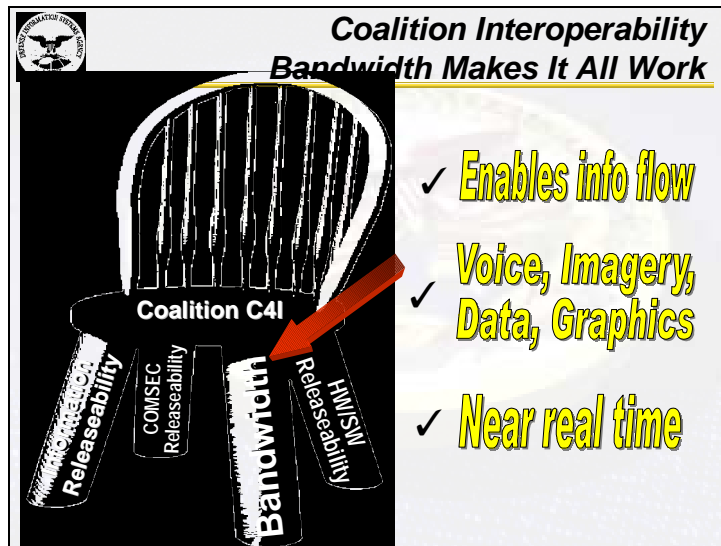


Figure 14

**Student:** The media this week have reported commercial pressure on the U.S. military to give up bandwidth for mobile phones. Does DISA get involved in that, or is that more SPACECOM or NSA or someone?

**Raduege:** We get into it big time. In fact, DISA put together the entire report for the DOD that took into account all the Army-Navy-Air Force-Marine space equipment that would be affected by the sale of some of those precious pieces of spectrum on the commercial market. That report was submitted to the OSD, which then submitted it to the National Telecommunications and Information Administration in the Department of Commerce, which then had to wrap all that together and provide it to the Federal Communications Commission—to Michael Powell. We got our representation in, and there are some concerns there, because if you're going to ask us to move out of certain frequency areas there are associated costs.

Think about this. We have satellites up in geosynchronous orbit that have a certain frequency on them, and some of our satellites last for thirty years. A couple of years ago, when I was at SPACECOM, we decommissioned and super-synched FLTSATCOM 1 [Fleet Satellite Communications]. FLTSAT, which was a Navy communications device, was built to last for seven years, and it lasted for twenty-seven. When you get lucky and a satellite lasts for thirty years, you can't just fly up to geosynchronous orbit, which is 23,000 miles, with the Space Shuttle and change out the frequency on it. There are huge implications. It's not ground based. Don't let anybody think, "Oh, gosh, I can't have third-generation Internet service: I can't have my cell phone and my Internet and all that stuff because the doggone DOD is being an old stick-in-the-mud. They can give up that frequency."

What we're saying is, "If you're going to sell our frequencies and push us off, then at least cover our costs from the proceeds you're going to get so we can fix ourselves, because this is not our fault. Also, be willing to wait, because we have assets that our government has paid a billion dollars or more to put up there that are going to be affected if you take that frequency away from us."

**Student:** Also, not all frequencies are created equal, and if you move out from the band of frequencies we're talking about, you actually lose capability. Industry wants those frequencies for the same reasons we want them: mobile communications.

**Raduege:** Absolutely.

**Oettinger:** That's one of the reasons for urging you in your term papers to look at these things through the lenses of the involved parties. Who will win this argument will depend on who has the greatest influence over Congress at the time and on whether the national security considerations outweigh the commercial considerations in the minds of the 435 representatives or 100 senators.

**Raduege:** These are very real concerns. I could argue the side of the commercial enterprises. I understand their perspective, because it's the economy, it's jobs, it's market share, it's world influence, it's economic security.

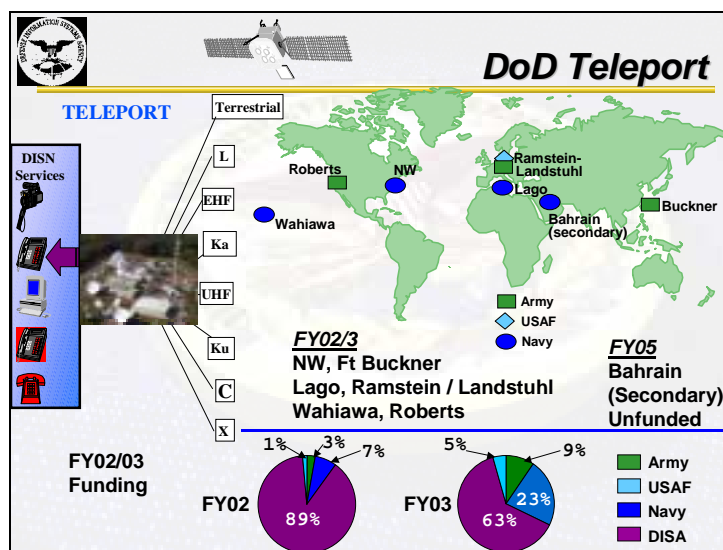
**Student:** I read a report that Verizon is spending millions on a lobbying effort to get military bandwidth.

**Raduege:** Right. Guess what? The DOD doesn't really do lobbying like they do, because it would be unethical for us. Legally, sometimes other people have somewhat looser standards.

**Student:** What's your endgame? Would you rather get paid for the change when those satellites de-orbit and give up those frequencies, or would you rather keep them?

**Raduege:** We'd rather keep our frequencies because of the long-term implications. It's expensive to turn off a satellite that you were fortunate enough to have, especially after all the expense of putting it up there. Going to geosynchronous orbit usually takes a huge booster. It's a quarter of a billion dollars just to launch the thing, not even including the payload. To think that you've got to turn it off and then super-synch it—throw it away—and replace it with something with a new frequency, boy! That's a lot of money! If you're going to do that, you're going to have to pay, because nobody's budgeted for that kind of thing. We haven't put that in our budget, and that's an expense. You have to weigh economic security against national security, and some of this involves national security. You could talk about the spectrum issue for a week, and there are lots of people doing it right now.

The DISN services provide users with secure and interoperable communications (**Figure 15**). These services include both classified and unclassified voice, video teleconferencing, and data networks; they're shown on the left of the slide. Integrated satellite and terrestrial DISN services have been, and continue to be, crucial in every contingency.



**Figure 15**

One of the main ways we use DISN to connect deployed forces globally is through our Standardized Tactical Entry Points. These STEP sites, as we call them, provide an easy plug-in communications path. Future operations will also connect to the DISN via an enhanced version of the STEP site called a teleport.

The STEP sites right now use X-band, satellite, or super-high frequency. In the future, we're going to expand these STEP sites and build all the other frequency areas shown on the slide, including global fiber and terrestrial means, and put it all into a site that looks sort of like

the one in the picture. We're going to have six of these sites, located at the places shown on the map, to allow expeditionary or deployed forces to use any one of the means I listed to get back to one of these sites and then back into all the huge computing services we provide here in the CONUS. We're no longer going to deploy all the forces forward; we're going to have them reaching back for these services through the teleport locations. We've got these sites under development right now; we're also going to put one in at Bahrain. Teleports extend our infrastructure to expeditionary warfighters, while our backbone upgrade magnifies the bandwidth leg of our coalition C4I chair here at home.

Here's a view of DISN today (**Figure 16**). We are introducing an additional 150 asynchronous transfer mode [ATM] points of presence and bandwidth managers to provide our networks with 64 times more bandwidth than they have today.

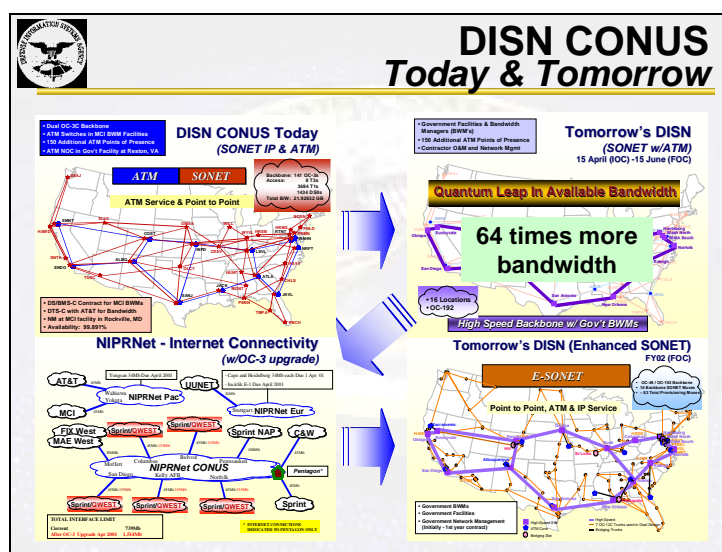


Figure 16

The capacity of the NIPRNet [Nonsecure Internet Protocol Router Network]—our unclassified DOD intranet—has increased by approximately 500 percent over the last two years. We all know how much more we use the Internet. The slide shows what that increased use translates into in the DOD in terms of what my engineers have had to try to program for, get out in front of, and provide. That's really significant. Our engineers have done a good job of anticipating NIPRNet growth and planning for it properly. We currently run at a 75 percent load during peak traffic periods, which provides us limited inherent surge capacity. We have ongoing efforts to ensure substantially more NIPRNet surge capacity. We are doubling NIPRNet capacity from 739 megabits to 1514 megabits. The backbone is moving quickly to OC-192, providing 10 gigabits per second of data throughput, so you can see how exponentially our bandwidth demands are growing. It's easy for you to understand, because we all demand more information in our personal lives today, and that's translating right into how we do DOD business.

**Student:** Will you be selling those services, or renting out bandwidth when you're not using it? Or would that be a threat to your network?

**Raduege:** I'm only leasing them out, or actually selling the services, within the DOD.

**Student:** Do you own the networks? Do you lay the fiber?

**Raduege:** We buy the service from Global Crossings, MCI, Sprint, and AT&T. We don't own the fiber, because that's infrastructure, and I don't want infrastructure. I want to pay a service provider to keep up that infrastructure. They're responsible for that.

**Student:** Let's say that MCI goes bankrupt, and Deutsche Telekom buys it. What would happen the next day? Would you rent from Deutsche Telekom? What are the implications?

**Raduege:** That's a hard question and it would depend on the particulars of the contract and the nature of the acquisition. This is particularly true where security clearances are involved. If the new owner can't meet the security requirements, such as personnel and facility clearances, I'd go to another provider.

When a foreign-owned company buys a U.S. company and there are security implications, the foreign company will usually set up a proxy committee composed of people whom we know very well. I had this happen to me not too long ago. A couple of retired four-star generals came into my office and said, "Hi! You can't announce this, but we are going to be purchased by a foreign company. However, we will be the ones who will handle your business and all U.S. business, because of the classified implications. It will go no further into the foreign company, and we will assure you of that." It's sort of interesting.

**Student:** And that's trustable?

**Raduege:** They usually put people in front of you for these committees or boards whom you know from background and experience. It tends to be a matter of trust to a certain extent, but there are also filings required that lay out "arms-length" business practices. The arrangements are negotiated and approved through the Defense Security Service. The new company is contractually bound to ensure it meets these requirements, or it loses the clearances and the contracts. You have to keep in mind that we regularly use international vendors to carry a lot of U.S. traffic overseas, but we protect that traffic through encryption and other contractual requirements.

**Oettinger:** I think it's essential to underscore the importance of trust. It cannot be overstated. You've heard him say this several times, once in connection with sharing information with Britain, Canada, Australia, and New Zealand and now in connection with this kind of firewall in a foreign acquisition. There are a lot of issues where trust plays a central role.

**Raduege:** I'm getting the signal here to speed up or I'll get the hook, so let's continue on DISN CONUS. We're going to continue to build this system. In other words, we've always got to be in front of the demand, and satisfy it.

As you can see, our \$238 million dollar DISN Expansion Program will significantly upgrade the DISN CONUS backbone (**Figure 17**). It equals the best commercial bandwidth available, and you can see that this expansion is the largest jump in military communications capacity in history. We're putting this upgraded system in across the CONUS now, and as of April 21, 2001, it's going to be turned on for our users. This represents huge amounts of bandwidth. So, when I said "Reach back to us, and we'll provide you the bandwidth and connectivity," these are the facts behind the words. This is big business.

Let's talk about security, our other focus area today. We look at the future with hope and concern: hope for peace in the Middle East, Chechnya, central Africa, and Kosovo (to name but a few places), and concern that virulent nationalism, organized crime, and the persistent cancer of terrorism will continue to present a challenge to our nation, its citizens, and our military forces. Our newscasts are plagued by stories about social unrest, refugees, terrorism, and the fearful but real possibility of the proliferation of weapons of mass destruction.

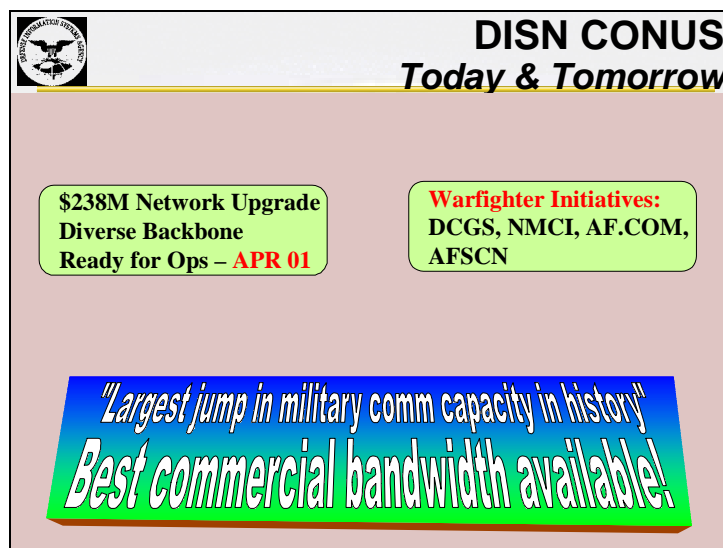


Figure 17

Our world is changing. Scientific advances and reliance on information technology have created a globally interconnected community. These technological advances are closely watched by a number of world actors. For example, consider the following quotation: “Information warfare will be the most complex type of warfare in the twenty-first century, and it will decide who will win and who will lose the war.” This thought does not come from a U.S. strategist; it comes from Chang Menxiong’s essay on “The Revolution in Military Affairs Weapons of the 21st Century,” which first appeared in *China Military Science* in 1995. It has recently been included in the compendium titled *Chinese Views of Future Warfare*, a doctrinal view of China’s People’s Liberation Army.<sup>14</sup> We are not the only ones who recognize the importance of information technology and that it can, and will, play a leading role in future conflicts.

You’re probably wondering what this picture is all about (**Figure 18**). No, it’s not a screen-saver of my kids—there’s a true story here. This is a screen capture of a recent, actual event. What you see here is a captured image of a computer desktop. The black spots at the left corner are the program icons that we blacked out.

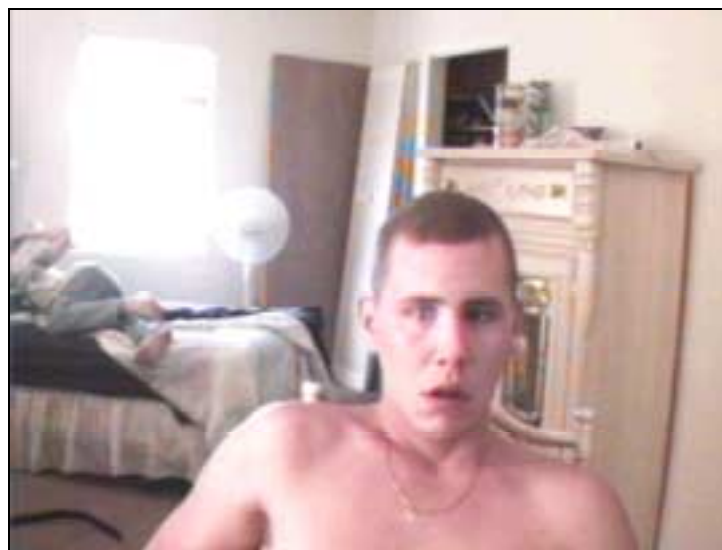
Imagine that you’re at home, sitting in front of your PC in your bedroom, chatting on your Yahoo! messenger with a friend. Next thing you know, a Microsoft alert box pops up, saying, “Hi, I know we haven’t talked before. This is your computer. Since I see everything in your room, I thought I’d throw you a few pointers. First, put on a shirt. PLEASE. Second, you’ve got a nice

<sup>14</sup>*Chinese View of Future Warfare*, edited by Michael Pillsbury (Washington, D.C.: National Defense University Press, 1997).

girl lying there on your bed, and you're sitting there looking like a goon on the computer. Come on!" Can you imagine how your face would look if you ever read a note like that from your computer?! Let me show you how this guy's face looked after his computer "talked" to him (**Figure 19**). A hacker took over this person's computer, spied on him via his Web cam, decided to have some fun with him, and even took a snapshot to remember—which law enforcement later confiscated. This case is currently in legal channels.



**Figure 18**



**Figure 19**

Let's put this case in perspective. Think about your offices and your homes! This was only one hacker at home. If one amateur hacker can exploit this knowledge, can you imagine what a



coherent program headed by several Ph.D.s with the resources of a nation-state could accomplish?

These are some of our concerns today (**Figure 20**). Our information networks face an increasing asymmetric threat ranging from nation-states to terrorist groups, from spies to organized criminals to hackers. From the most common hacker attacks to the least frequent—but most dangerous—state-sponsored attacks, the threat is evolving, and the tools are getting more powerful. Teenage hackers, once viewed as nonthreatening and purely recreational, now can significantly disrupt commercial networks. What Robert Morris started back in 1988 by releasing his computer “worm” virus into the Internet has matured into a far more devastating threat today. In fact, last July, a Price Waterhouse Coopers survey of 50,000 U.S. firms estimated the cost of software viruses at \$266 billion—2.5 percent of the nation’s gross domestic product—and nearly equal to our defense budget. The estimated worldwide cost reached \$1.6 trillion.

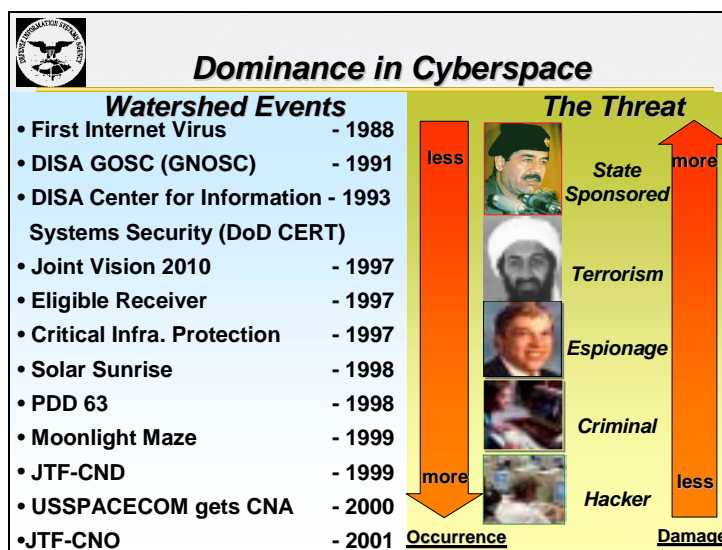


Figure 20

DISA first addressed this escalating threat a decade ago by creating the Global Operations Security Center [GOSC], known today as the Global Network Operations and Security Center [GNOSC], which provides network situational awareness across the DOD. We continued to evolve, and in 1993 created the Center for Information System Security, the precursor of today’s DOD CERT [computer emergency response team].

Although the Joint Staff’s vision of 2010 didn’t identify a single DOD “bellybutton” for information assurance, it recognized the potential of the information revolution. We saw first-hand the importance of the information revolution during our own Eligible Receiver exercise in 1997, which revealed serious vulnerabilities in our information systems. The need for protection was highlighted later that year, when the president formed the Commission on Critical Infrastructure Protection. The vulnerability of our networks was further underlined in 1998 when two U.S. high school kids and “The Analyzer,” a hacker from Israel, disrupted our information networks, and then again when hackers, apparently operating from Russia, raided unclassified

government computer networks in what became known as Moonlight Maze. We found we could no longer treat hackers as just a nuisance.

These malicious criminal acts accentuated the importance of Presidential Decision Directive 63, which published the National Critical Infrastructure Protection Plan and established the National Infrastructure Protection Center. The Joint Task Force for Computer Network Operations [JTF-CNO] is the DOD's parallel to the National Infrastructure Protection Center. As most of you know, DISA teams with USSPACECOM and the JTF-CNO to defend all DOD networks. Our GNOSC provides direct support to the JTF through our DOD CERT and is poised to stand up a crisis action team whenever necessary.

Effective computer network operations require a partnership among network operations, law enforcement, and intelligence, with operational leadership. USSPACECOM's assumption of the CND and CNA [computer network attack] missions reflects the DOD's commitment to these vital requirements. DISA's commitment to assisting USSPACECOM is firmly anchored in more ways than one. Major General Dave Bryan, DISA's vice director, is dual-hatted as the commander, JTF-CNO, and in that role works directly for General Ed [Ralph E.] Eberhart, USCINCSpace.

This chart is one I wanted to get to (**Figure 21**), because these are some of the statistics that we were talking about over lunch. Operations within the information domain have become as important as those conducted in the domains of sea, land, air, and space—inextricably linked to focused logistics, full-dimensional protection, precision engagement, dominant maneuver, and joint command and control.

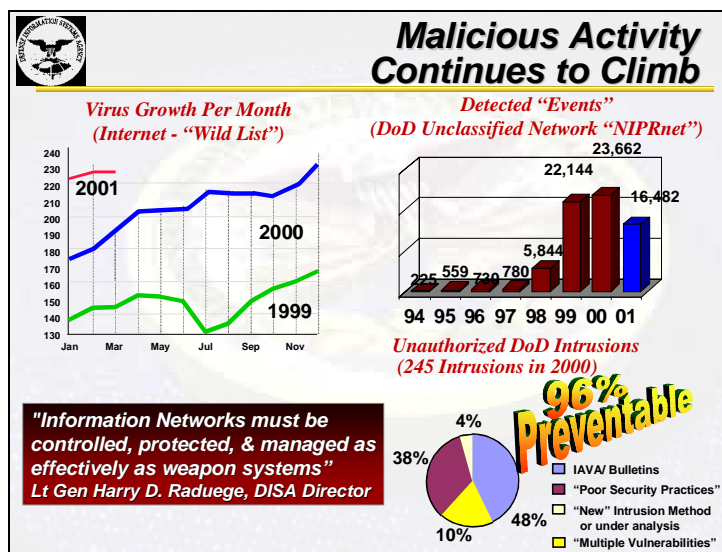


Figure 21

At DISA, "Networks-R-Us," and they have been for forty years, as I showed you on my first slide. We are adapting to the speed of change in IT and to the evolving threats. In fact, we fully understand that DOD information networks must be controlled, protected, and managed as effectively as weapon systems.

Our information networks are under constant attack. For example, a few weeks ago, we recorded one organization that scanned one of our network servers over 7 million times in one day—and this is not at all an uncommon event. The top left part of the chart, showing virus growth on the Internet per month, hit 225 during March 2001, up 85 percent from March 2000. Look at those increases in the number of viruses! This is incredible! Some of the big ones are the ones we hear about on CNN or that you get on your home computer, such as Melissa and “I Love You.” This is how active it really is. This is what we’re seeing on the Internet, and this war is happening on a daily basis.

The upper-right graphic illustrates more serious intrusion attempts, and clearly shows a steady increase in malicious activity during the year 2000—an increase of nearly 7 percent over 1999. So far this year, we’ve had 16,482 “detected events,” well above where we were this time last year. The large increase, however, can be attributed to several things: our new, more comprehensive automated reporting method, better sensor monitoring, or increased activity.

The bottom-right chart shows that during the year 2000 we experienced 245 unauthorized root- and user-level accesses, the most serious of incidents. That’s more than double 1999’s incidents. However, implementing published IAVAs, or information assurance vulnerability assessments, and following established security practices could have prevented the vast majority of these. We’re talking discipline! Sometimes it’s just as simple as not using a dictionary word, which can be discovered quickly, as your password. Computers these days can scan dictionaries in seconds and find your password.

Malicious activity against our networks continues to rise. To stay ahead of the curve, we’re changing our posture from reactive to predictive and continuously improving our network monitoring capabilities.

Here’s an example of one of the reasons we believe we’ve seen an increase in activity (**Figure 22**). You no longer need a total understanding of the tools and ways to employ them to attack a Web site. All you need to learn is how to point and click. This Web site was utilized

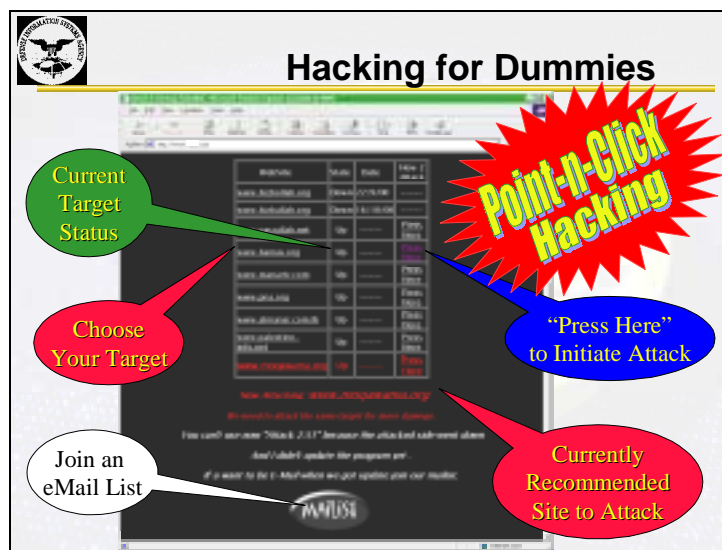


Figure 22

during the recent Palestinian–Israeli conflict. In this case an Israel sympathizer created a site to attack Hezbollah, Palestinian, and Hamas Web sites. From recommended targets to an e-mail list—in case you would like to learn more—it’s all done for you. Just point, click, and hack.

In his book *On War* (1818), Lieutenant Colonel Carl von Clausewitz said: “If you entrench yourself behind strong fortifications, you compel the enemy to seek a solution elsewhere.” His words could just as easily be applied to computer network defense as to the earthen trenches that were designed to defend France from an attack by Germany. The Nazis easily overtook those static defenses. Fortifications, much like computer firewalls, are designed to keep your infra-structures safe, but these static defenses alone do not work. They just “compel the enemy to seek a solution elsewhere.” I would love to have this lieutenant colonel on my information assurance team.

Firewalls provide some measure of protection, but, as Clausewitz reminds us, we need much more than that. We need an integrated IA team to defend our networks (**Figure 23**). DISA’s day-to-day guardian of the DOD networks is the GNOSC that I mentioned earlier. DISA’s GNOSC provides worldwide network monitoring, contingency support, network crisis action support, network resolution management, and network–IA integration. It also houses the DOD CERT, the technical arm of USSPACECOM’s JTF-CNO, which is collocated with the DISA GNOSC.

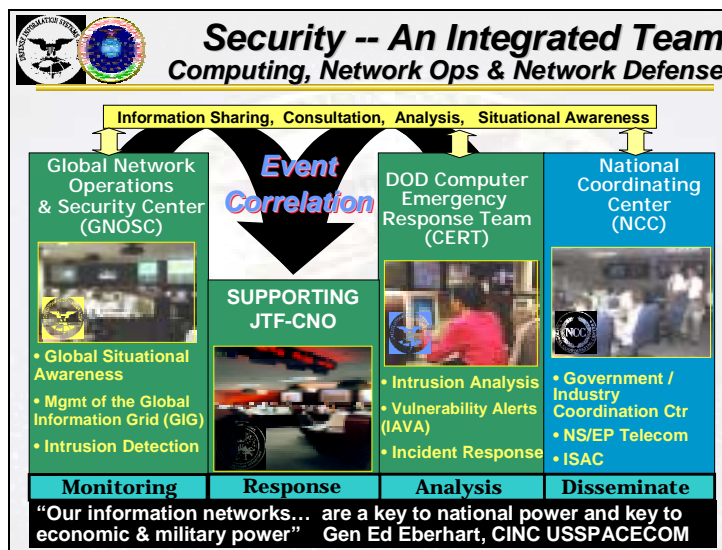


Figure 23

The far right of the slide shows the National Coordinating Center [NCC] of the NCS, my second hat. The NCC, a joint industry-government center, coordinates initiation and restoration of telecommunications services during national emergencies. In partnership with others in industry, the NCC has established an ISAC. Through this cooperative effort, we are taking the bold step of putting our NCC into the prediction business, enabling us to react at the first indication of trouble—alerting our partners and calling in the cavalry before a problem becomes a disaster. As a first step, we are establishing an NCC watch officer and desk to be collocated with the DOD

CERT, GNOSC, and JTF-CNO. This move will significantly enhance our ability to alert government and industry partners to pending cyber issues.

Deploying and maintaining a robust and effective sensor grid to detect intrusions is essential to protect the DOD's Global Information Grid (**Figure 24**). Command and control networks, services, applications, and infrastructure components across the GIG must be protected. We are integrating existing sensor technologies into a cohesive infrastructure. The Joint Intrusion Detection System is DISA's proven tool for network-based intrusion detection, analysis, and monitoring across the GIG, and it's an integral part of our defense-in-depth strategy.

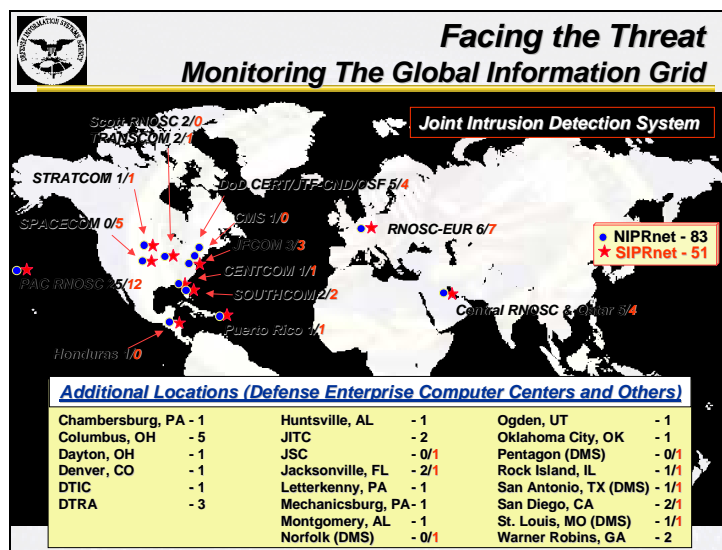


Figure 24

We at DISA are living up to our DOD-directed responsibilities as the “technical integrator” of the CND sensor grid. In fact, we currently have a project under way with USCINCPAC to provide 100 percent coverage of PACOM's theater networks. PACOM isn't the only theater where we've implemented a more robust network monitoring capability. This slide shows DISA's global IA presence and where we've installed our Joint Intrusion Detection System throughout the DOD NIPRNet and SIPRNet (Secret Internet Protocol Router Network) around the globe. We've also increased monitoring of our regional STEP sites and critical C2 enclaves.

Today, each military service has its own sensor grid, and DISA provides a sensor grid as well. To achieve the vision of information superiority, as outlined by our Joint Staff, we must be prepared to take the next step, which is to create an enterprise sensor grid with common attributes. We need a shared view of sensor status keyed to locations. This means a collaborative process to share signatures and vulnerabilities, so all incidents are detected and reported consistently. We also need a DOD-wide procurement strategy to maximize economies of scale in purchasing sensors. We must move forward to correlate information from our existing disparate sensor grids into a fully integrated CND sensor grid.

Above all, we must remember the deployed warriors when establishing and professionalizing the Joint Staff defense-in-depth vision (**Figure 25**). Now more than ever, our expeditionary forces require the right information, at the right time, and in the right format. We're

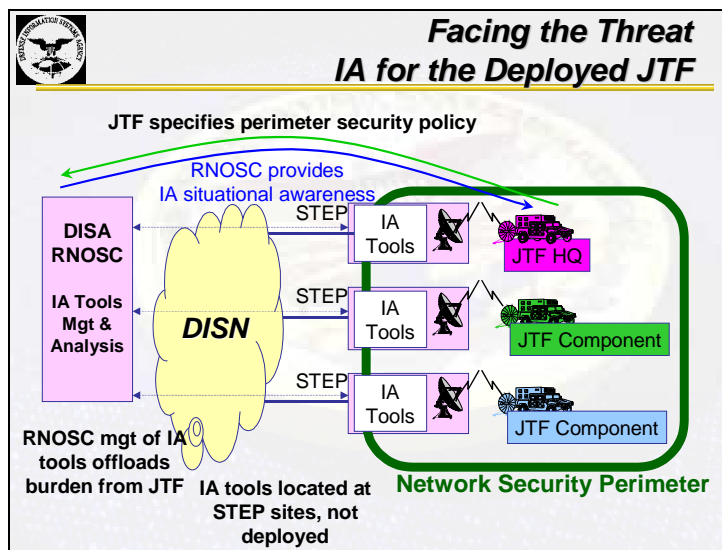


Figure 25

committed to providing those at the tip of the spear with our DISA core competencies of joint interoperability, assured security, and best value. We have already experimented with IA tools in the JTF environment of Southwest Asia, and we've learned the benefits and challenges associated with integrating IA at this level.

To attain and preserve information superiority, we must provide a secure and interoperable global information environment at the user, server, and application layers (Figure 26). Our PKI initiative creates a flexible asymmetric system that allows public key-enabled applications to interoperate securely. The joint PKI team of DISA and Mike Hayden's NSA have made great strides by going operational with the DOD PKI on the NIPRNet in July 2000.

The complex block, titled "Raising the Bar Public Key Infrastructure", contains a bulleted list of PKI capabilities and partnership goals. The list is as follows:

- What PKI does:
  - Data Integrity: Protection from undetected modification
  - Data Confidentiality: Protection from unauthorized disclosure
  - User Identification and Authentication: User identity verification
  - Access Control: Protection from unauthorized use
- Way ahead for DISA/NSA PKI Partnership
  - DoD PKI operational now on NIPRnet **Done**
  - Have Key Escrow/Key Recovery capability now
  - Begin certificate issuance on Common Access Card
  - Evolve the PKI in line with current policy

An illustration of a person climbing a bar is on the right side of the list.

Figure 26

If we are to maintain our technological high ground, we must continue to professionalize the force (**Figure 27**). At the beginning of the year, the deputy secretary of defense signed a DOD directive outlining the requirement for each CINC, service, and agency to provide adequate local-enclave CND services linked to our existing CERT structure. DISA's role is to standardize, professionalize, and institutionalize CND services. This process is still under construction, but I want to give you a peek at what we're developing, so you can see first-hand how we're going to standardize and professionalize the execution of the DOD CND. Our goal is to establish a standardized process that provides a means to help CND services providers improve productivity and meet client expectations.

The slide features the Department of Defense seal in the top left corner. The title is "Facing the Threat Certification and Accreditation". Below the title, the section is "DISA Responsibilities". The list includes: "Standardize and professionalize DoD CND execution", "Certification Authority for Secret & below CND Services (CNDS) Providers", "Provide CNDS support to DoD Components", "Advisory Alert & Tech Support", and "DoD CND System Integrator". At the bottom left, it says "LEADERSHIP & DISCIPLINE". On the right side, there is a graphic of a hand holding a certificate with the "CNDS CERTIFIED" logo.

**Figure 27**

DISA will also provide CND services support to DOD components that don't subscribe to other CND service providers. This capability covers DOD agencies and activities not already covered by a CINC or military service CERT and helps ensure comprehensive CND coverage of DOD networks. We will also establish advisory and alert procedures for CND providers and continue to provide JTF-CNO with technical alert support. Additionally, we'll provide subscribing CERT components and the JTF-CNO with trend and pattern analysis support. We're committed to continuing our efforts to provide the DOD with integrated CND-related systems.

We not only provide our partners with the right information on-time, every time, but we also do so with assured security. Dick [Richard A.] Clarke, national coordinator for security, infrastructure protection, and counterterrorism within the National Security Council, reminded us in a speech last December that hostile or potentially hostile organizations "are doing reconnaissance today on our networks, mapping them, looking for vulnerabilities." In a world where our DOD networks are probed millions of times every day, how can we separate which network events are truly important from those that aren't?

The future of IA requires that we advance in terms of both people and technology (**Figure 28**). Only then will we make progress on the operational front. Ideally, we'll have automated detection, real-time shared situational awareness throughout DOD, and IA fully operationalized



Figure 28

and integrated into the commander's view of the battle. I'm confident we'll get there, but today we must answer the commander's question: "Am I able to execute my mission, given the state of my supporting information infrastructure?"

To assist us in this effort, we're transitioning our Automated Intrusion Detection Environment—or "AIDE"—from an advanced concept technology demonstration to an operational capability. AIDE will monitor a constellation of rule-based sensors strategically located throughout the DOD's Global Information Grid. AIDE also allows real-time alerting and monitoring of malicious network activity. More than just detecting and reporting, it will also help us analyze suspicious behavior.

Situational awareness of IA is a critical capability. Commanders need visualization tools to view the health and welfare of their networks. We must continue working on interim architecture components that allow other sensors to "plug in" and present a true, integrated IA picture. IA situational awareness of IA should also include CNA indications and warning, traditional threat data and analysis, automated patternless detection, alerting, and forensic data collection.

As you know, technology alone can't produce an IA panacea. As is clearly stated in our defense-in-depth strategy, people play a vital role. I had the opportunity to attend the IA Workshop at Norfolk, Virginia, this February. What a great group of professionals! If one theme permeated the entire workshop, it certainly was, "As we share our networks, we also share the risk." We share the risk with our DOD community, and we also share the risk with our strategic industry partners. Protecting our networks is a strategic partnership—a partnership among industry, the DOD, and the rest of the federal government.

Few know this better than the leadership of the NCS, the second "hat" I wear (**Figure 29**). The NCS was born out of the Cuban Missile Crisis and continues today to build on its rich history, partnering with industry and government to keep the nation's emergency communications effective, secure, and interoperable. As we discussed before, the NSTAC remains strong, with thirty senior IT industry executives. We also house the NCC, which runs the government and





**Figure 29**

industry telecommunications ISAC I mentioned earlier. Our telecommunications ISAC was the first of its kind to stand up, and it has been lauded as a model for others to follow.

Recently, we incorporated an analyst from the U.S. CERT Coordination Center at the Carnegie Mellon University Network Survivability Organization into our GNOSC and DOD CERT to gain further synergy with industry. We also recently participated in White House initiatives on critical infrastructure protection to address the proposal for creating a cyber warning network—a future look at voice and data networks for national security and emergency preparedness.

The British statesman and philosopher, Edmund Burke, captured my philosophy on our current increasing cyber threat. He said, “He who wrestles with us strengthens our nerves and sharpens our skill. Our antagonist is our helper.” As individuals and as a nation we are getting better at protecting our critical national infrastructure.

**Oettinger:** I’m going to get drawn and quartered by the next class if we don’t vacate this room by 4:00, so I’m afraid I have to ask you to wind up your presentation. This was a virtuoso performance for which we are enormously grateful. We have a small token of our large appreciation.

**Raduege:** Thank you! I really appreciate it.

## Acronyms

AIDE	Automated Intrusion Detection Environment
APAN	Asia–Pacific Area Network
ASD C3I	assistant secretary of defense for command, control, communications and intelligence
ATM	asynchronous transfer mode
C2	command and control
C4	command, control, communications, and computers
C4I	command, control, communications, computers, and intelligence
CCEB	Combined Communications-Electronics Board
CENTCOM	U.S. Central Command
CEO	chief executive officer
CERT	computer emergency response team
CINC	commander in chief
CINCPAC	commander in chief, U.S. Pacific Command
CNA	computer network attack
CND	computer network defense
CNN	Cable News Network
CNO	computer network operations
COE	common operating environment
COMSEC	communications security
CONUS	continental United States
COP	common operational picture
COTS	commercial off the shelf
CSE	combat support enhanced
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information Services Network
DOD	Department of Defense
FEMA	Federal Emergency Management Agency
FLTSATCOM	Fleet Satellite Communications
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GIG	Global Information Grid
GNA	Goldwater–Nichols Act
GNOSC	Global Network Operations and Security Center
GOSC	Global Operations Security Center
IA	information assurance
ISAC	Information Sharing and Analysis Center
IT	information technology

JTF	joint task force
NATO	North Atlantic Treaty Organization
NCC	National Coordinating Center
NCS	National Communications System
NIPRNet	Nonsecure Internet Protocol Router Network
NMCI	Navy–Marine Corps Intranet
NSA	National Security Agency
NSTAC	National Security Telecommunications Advisory Committee
OSD	Office of the Secretary of Defense
PACOM	U.S. Pacific Command
PC	personal computer
PKI	public key infrastructure
SIPRNet	Secure Internet Protocol Router Network
STEP	Standardized Tactical Entry Point
USAF	U.S. Air Force
USCINCSpace	commander in chief, U.S. Space Command
USSPACECOM	U.S. Space Command
WAN	wide area network



INCSEMINAR2001



ISBN 1-879716-76-3