INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Improved Application of Information to the Battlefield—Revisited
Robert A. Rosenberg

Guest Presentations, Spring 2002
Robert B. Brannon, Gregory C. Radabaugh, Robert A. Rosenberg, Gary L. Salisbury, Roberta E. Lenczowski, James B. Plehal, Dean W. Cash, Patrick F. Kennedy, Warren B. Rudman, Joseph K. Kellogg, Jr.

August 2002

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 © 2002 by the President and Fellows of Harvard College. Not to be reproduced in any form without written consent from the Program on Information Resources Policy, Harvard University, Maxwell Dworkin 125, 33 Oxford Street, Cambridge MA 02138. (617) 495-4114

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-81-X **I-02-1**

August 2002

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

AT&T Corp.
Australian Telecommunications Users Group
BellSouth Corp.
The Boeing Company
Booz Allen Hamilton
Center for Excellence in Education
Commission of the European Communities
Critical Path
CyraCom International
DACOM (Korea)
Ellacoya Networks, Inc.
ETRI (Korea)
Fujitsu Research Institute (Japan)
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
Hitachi Research Institute (Japan)
IBM Corp.
Korea Telecom
Lee Enterprises, Inc.
Lexis–Nexis
John and Mary R. Markle Foundation
Microsoft Corp.
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
NEC Corp. (Japan)
NEST–Boston
Nippon Telegraph & Telephone Corp (Japan)
PDS Consulting
PetaData Holdings, Inc.
Research Institute of Telecommunications and Economics (Japan)
Samara Associates
Sonexis
Strategy Assistance Services
TOR LLC
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

Improved Application of Information to the Battlefield—Revisited

Robert A. Rosenberg

February 28, 2002

Major General Robert A. Rosenberg, USAF (ret.) is executive vice president and general manager, Washington Operations, Science Applications International Corporation (SAIC). Before retiring from active duty in the Air Force he was director of the Defense Mapping Agency (DMA) from 1985–87, and from 1983–85 he was vice commander in chief of the North American Aerospace Defense Command and assistant vice commander of Air Force Space Command. He served as assistant chief of staff for studies and analyses, Headquarters, USAF, from 1980–83, and from 1976–1980 was a member of the National Security Council (NSC), where he served as advisor to the assistant to the president for national security affairs. From 1974–76, Gen. Rosenberg served as deputy director for programs, principal deputy, and then acting director of the Office of Space Systems, Office of the Secretary of the Air Force. He has also managed the USAF Operations Research Center and served as U.S. delegate to the North Atlantic Treaty Organization (NATO) Advisory Group for Aerospace Research and Development. Gen. Rosenberg received a B.S. degree in general engineering from the U.S. Naval Academy, an M.S. in aerospace engineering from the Air Force Institute of Technology, and graduated from the Industrial College of the Armed Forces.

Rosenberg: My presentation today has almost the same theme as the one I gave when I was here in 1996.[1] That probably gives you some message, and that is "We're still trying, and we're still failing." We haven't made a hell of a lot of progress in some areas, and we have made a hell of a lot of progress in some areas.

You're going to see me look at some notes, because, although I'm very familiar with the topic, some of the details I want to talk to are not things I'm familiar with. If you get bored with what I'm saying to you, you can look at the notes and I hope that in some way they'll relate to what I'm going to talk about.[2]

---

[1]See Robert A. Rosenberg, "Defense Science Board Recommendations on Information Architecture for the Battlefield," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1996* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-97-1, January 1997), [On-line]. URL: http://www.pirp.harvard.edu//pubs_pdf/rosenbe\rosenbe-i97-1.pdf

[2]The talking points, and Gen. Rosenberg's slides, are appended at the end of his presentation.

I'm going to talk about some experiences that I personally have had over the last seven years or so working on a little special project for secretaries of defense and assistant secretaries for C3I [command, control, communications, and intelligence]. While the background information I'm going to talk from relates to three military operations over a five-year period in the Balkans, I'm going to assert as I go through all this that on the basis of what we have learned from our experiences in the Balkans in terms of the world of C2ISR [command, control, intelligence, surveillance, and reconnaissance], C3ISR, or C4ISR [command, control, communications, computers, intelligence, surveillance, and reconnaissance] (depending on which you believe is right), my comments are applicable to other military operations, including major regional conflicts [MRCs], even though MRCs aren't the currency of the day in the current administration. Nonetheless, we still have to be prepared to fight them.

The good news is that in all of these efforts, beginning back in 1995 in the Bosnia campaign, we made the information flow to wings, carrier battle groups, and divisions in the Bosnia, Kosovo/FRY [Federal Republic of Yugoslavia], and Afghan theaters much more robust, so we know that information flow can work well anywhere else and could be done worldwide if we had to. The only reason it works is that we continue to find that the American military, civilian, and contractor talent to get the near-impossible done when called upon by our nation still flourishes and excels with innovation and initiative…in spite of the limited resources we gave them, little time to plan or train, and political constraints that sometimes make it even tougher to succeed. In less polite circles, I say that they make it work in spite of the garbage we give them to work with. We're really lucky when we get youngsters on the battlefield and see how they take the trash that the older generation bought for them and actually can go off and make it work and win wars with it.

This personal experience I'm going to talk about relates to the fact that three weeks after the [Scott] O'Grady shootdown in June 1995 Secretary of Defense [William] Perry called me and four other guys into his office and asked us to go to the European theater. As he put it, "Every time I ask the intelligence community why O'Grady got shot down, I push and I get mush for an answer. Every time I ask why it took five-and-a-half days to get him back, I push and I get mush for an answer. I want you to go over to Europe and find out why. As a matter of fact, come back with recommendations for a sufficiently dramatic change in intelligence support to our warriors to make it a safe enough place to put 20,000 U.S. youngsters on the ground in Bosnia as a peace enforcement force."

The first thing I did that night when I went home was say, "Honey, Bill has lost his mind. He's crazy." She said, "He didn't ask for your political advice. He asked for your technical advice. That's a holocaust happening, and you have an obligation to help, so you're going to go."

One of the things you find is that you get what you pay for, so when people ask people to give advice to the government pro bono, they don't necessarily agree with the task. We told Bill he really didn't have the tasking quite right. We said, "It's probably not an intelligence problem; it's an information problem, and is much broader than national intelligence." So we changed our own terms of reference to say we wanted to look at the whole world of how information flows to warfighting forces.

As an important point of history, in case some of you wonder how our leaders feel about what we do with the young people of America when we ask them to go off to war, when Bill said to us, "I want you to make it a safe enough place to put 20,000 U.S. youngsters on the ground," this was a secretary of defense [SECDEF] who was personally and very emotionally committed to not losing a single life. He handed all of us a U.S. Army publication on the history of the German occupation in World War II, which noted that the Germans lost one in seven "peace-keepers" to guerrilla warfare in the Balkans. He said, "This is what you must not permit to happen. This is what I want you all to stop."

We got a lot of briefings in Washington, D.C. At the time Perry called us in, we were flying forty sorties a day that were unsuccessful in keeping twenty-one Bosnian Serb airplanes on the ground. They had decision dominance of the battlespace. They were inside our information cycle time. Twelve hours after we arrived in Vicenza, when we were sitting around a table with General Hal Hornburg, who was the NATO air boss, Snuffy [Leighton] Smith, the Navy four-star who was the Allied Forces South commander, called Hal and said, "We're going to start a bombing campaign in twelve hours to drive them to the peace table."

Some of you are familiar with how the government operates and understand things like Defense Science Boards [DSBs] and Army Science Boards and Air Force Science Boards (I kiddingly always refer to those as "opium-smoking studies") that get their studies put on a shelf. Ten years later some smart major pulls them out, dusts them off, says "Eureka!" and gets promoted below the zone for inventing something that we talked about ten years before. But in this case, as opposed to a typical opium-smoking DSB, we actually participated in a war. We were at Vicenza, where the strikes were planned; we were aboard a carrier from which combat operations were conducted; we were down at Aviano, where land-based air operated; and we were aboard a Navy command and control ship out in the Aegean Sea.

When we got back, after we had observed that bombing campaign in real time from carriers and command centers and so on, we made several recommendations to Secretary Perry, to John Deutch, who was the DCI [director of central intelligence], and to Bill Owens, who was the vice chairman of the Joint Chiefs of Staff [JCS]. Those recommendations resulted in Perry and Deutch standing up a joint DOD/CIA [Department of Defense/Central Intelligence Agency] team to implement our recommendations. We looked the SECDEF in the eye and we said, "If you don't do these things, don't put 20,000 U.S. youngsters on the ground, because you're going to lose a bunch of them." Over the ensuing months, before we actually went into Bosnia, we had monthly meetings with Bill and with a group co-chaired by Ken Minihan, who was the director of the Defense Intelligence Agency [DIA] at the time, and by Denny Blair,[3] who was the deputy to the DCI for military affairs. It was a unique experience as a contractor, sitting in judgment on my customers with whom my company had more than a few billion dollars at risk. It was an interesting situation, because I'm not known for being bashful about telling a customer when the hell he's wrong.

Oettinger: That's because you're not working for Arthur Anderson.

---

[3]Lieutenant General Kenneth Minihan, USAF; Admiral Dennis Cutler Blair, USN, currently commander in chief, Pacific Command.

Rosenberg: Tony's guidance to me was "Tell them what I really think they ought to know." Because many of you are in the government, it is important that you know, just as I felt when I was in the government, that the worst contractors I had were ass-kissing yes-men. Because they feared the loss of their business with me, they would always tell me what they thought I wanted to hear. The best contractors I had were the ones that said, "Rosie, you don't know what the hell you're doing!" So I'm fairly infamous for letting my customers know when they don't know what the hell they're doing. That pays off, because what most government contractors care about is successful government. We want to see our customers succeed.

As I said, we sat in judgment on a monthly basis, listening to what they were doing to prepare to go into Bosnia, and, finally, when we went around the table at our last meeting, I looked at the SECDEF and I said, "I would not be afraid to send my three adult children over there as part of the peace enforcement operation." That's how much confidence I had in the things that we had done. As I go through this presentation, we're going to talk about some of those things. There really were major changes that took place.

I met with a smaller group of you at lunch, and we were talking about security impediments to military operations. Some of you aren't old enough to remember the Bosnian war, but several weeks after the O'Grady shootdown a French aircraft got shot down. We were in San Vito with the two SOF [special operations forces] helicopter crews that were planning the recovery of the downed French pilots. As part of our outbriefing to Secretary Perry and Dr. Deutch, we laid on a conference table the one lousy photograph that those helicopter crews had of the battlespace where that downed French airplane was and where we were going to have to send kids to put their lives into danger so they could recover our allied friends. For those of you who understand intelligence imagery, and know what NIIRS is—the National Imagery Intelligence Rating Scale—a NIIRS 9 is a good as it gets. That's high-definition TV. A NIIRS 0 is as crappy as it gets. We put this one picture in front of Secretary Perry, and we said, "This piece of crap, this NIIRS 69 photograph, is all these young warriors had in their hands and it took forty-five minutes, Mr. Secretary, for them to get it over 9.6 kilobit telephone lines, because their DSCS [Defense Satellite Communications System] terminal was down, and you sure wouldn't waste good communications on warriors, would you?"

Next to that one lousy photograph I had also laid out all of the EOIR [electro-optical infrared] radar and every other marvelous piece of information they had in Washington, D.C., of that same battle scene. I said, "Bill, this is a criminal act. There's no reason why you and the president and [National Security Advisor] Tony Lake and [Secretary of State] Warren Christopher shouldn't have this, but there's also no reason why the kids whom you are willing to sacrifice in the name of freedom shouldn't have it also." Up until that time, there were all kinds of restrictions on how we could get national foreign intelligence information into the hands of our warfighters. Some of them were bureaucratic restrictions, some of them policy restrictions, some of them communications restrictions, and some of them artificial restrictions created by something we call "sources and methods."

In one fell swoop, a national policy decision was made when Bill Perry looked at John Deutch and said, "Don't you think that's kind of ridiculous?" We said, "You need to change from cold war systems-high security to modern world systems-low, where you understand that every time we fail to share information with coalition partners we put our own forces at risk because

we're operating from a different sheet of music. Every time we overclassify information and don't put it into our own warriors' hands, we risk their lives too." As a result, they made a policy decision that resulted in approximately 90 percent of all National Foreign Intelligence Program information, both from the world of SIGINT [signals intelligence] and from the world of imagery, going out to 33 coalition partners at the Secret IFOR [Implementation Force (Bosnia)] level during the IFOR operation.

Oettinger: Let me develop that point with just a little bit of personal history. You're all aware that Dean Clemons is here as an Air Force national defense fellow. That relationship with the Air Force was started when Rosie was in the Air Force chief of staff's office, and he hitched us up with the Air Force and a succession of fellows. The reason that's relevant here is that one of your readings a little bit later in this semester will be a book by Martha Maurer, who was one of Dean's predecessors as the Air Force national defense fellow.[4] Her book is all about coalition warfare. She took her career in her hands in developing that book, because during the time when she was working on it here that was an unmentionable.

I'm just trying to put in context the absolutely radical change in policy outlook that Rosie has described, with the DCI and the SECDEF saying, "We're going to play coalitions," because, as he says, coalitions are a way of life. When you read Maurer, put yourself in the context where to keep her safe, and in fact to get her to dare to do research and write the damn thing, Rosie's former boss Jasper Welch,[5] who was by then retired, had to be dragged out to inspire her and promise her protection, because touching the subject of coalition warfare was a no-no that could be dangerous to somebody's career. Am I exaggerating?

Rosenberg: No, but I'm going to leap ahead and tell you that by the time we got to Kosovo we totally reversed what we did in IFOR, and we had seven separate classification systems. We didn't make a breakthrough, or we made a breakthrough for a short time.

Somebody asked me during our conversation at lunch how this multiple-level security thing is going. It depends on what's at stake. I tried, though I probably didn't get it across very successfully, to give you a feeling of the emotion in Secretary Perry's heart and head when he realized the burden of turning to the president and saying, "It is safe enough to put 20,000 kids on the ground over there." There was a lot at stake, and they didn't have a big NSC meeting to debate this nonsense; they just did it. Later on, in Kosovo, things were different, and we'll get to that.

I want you to understand Washington, D.C. When I first went to the White House, I was preparing a decision paper for President Ford as the intelligence wienie in the NSC. (I always refer to people on the White House staff as "White House wienies," lest they think they're very important, like that idiot Ollie North thought he was. My job included the same functions Ollie had, except I think I did it honestly.) As I was preparing that paper, I asked "Whom do I co-ordinate this with?" Everybody else was too busy and I found, "Oh, my God, this paper is going to go from me straight through Brent Scowcroft to the president." (Again, probably of more value

---

[4]Martha E. Maurer, *Coalition Command and Control* (Washington, D.C.: National Defense University Press, 1994).

[5]Major General Jasper A. Welch, USAF (ret.), former USAF assistant chief of staff for studies and analysis.

than my briefing is to share some of these stories.) I got a phone call from Brent Scowcroft's secretary saying, "Rosie, get over here to the West Wing. Brent needs to see you." I was a colonel, so I trudged across the street from the Old Executive Office Building. He was busy writing, and he held up this twenty-page decision paper I had written, and he said, "Rosie, get this down to less than three pages, will you?" "Brent! Impossible! This is the most important intelligence decision President Ford is going to make in his term in the White House!" He looked at me and said, "Colonel, if you can't get this down to fewer than three pages, go back to the Pentagon. I don't need you here."

That was an important message. All of you are in your mid-careers. Wherever you go, at least for a while, there's going to be somebody above you whom you're going to be helping, and that person doesn't have time to waste separating the fly feces from the pepper. That's your job. That's what you're paid to do, so do it! You will be far more successful, rather than wasting your boss's time with twenty-page papers. So I went back and bent to the task, got rid of all the Rosenberg baloney, and got it down to three pages. That paper led to the creation of Executive Order 11905, the so-called reform of the intelligence community in the aftermath of Watergate.[6]

At any rate, I've recapped a little bit about that first trip to Bosnia. A very important thing to share with you is that when we sat at the table at Vicenza it was a NATO meeting. The trip was advertised as a NATO meeting, and then we were all going to run off inside the concertina wire to a U.S. national SCIF [special compartmented intelligence facility]. General Hornburg had all the NATO air bosses sitting around the table (remember, this was before the air war started). We went around the table, and each person introduced himself and made some comments. The Dutchman said, "Go back home and tell your president and your secretary of defense you have no right to assert a leadership role here!" We went on around the table, and General Hornburg said, "Thank you very much, gentlemen. If nobody has any questions that's the end of the meeting." I said, "Wait a minute, Hal. Colonel, how about amplifying what you meant?"

The Dutchman said, "General, you make a national hero of this inept O'Grady fellow, whom we would have court-martialed for his ineptness. He laid on his own antenna for seven days, and he didn't properly train himself for battle. More important, you don't have the guts to be the leaders. Over the past five years here in the Balkans, we have had 130 comrades killed in action and 1,300 wounded, and you think it's a national disaster if you lose one person. You're not qualified to lead this operation. In the Dutch air force, we fly RF-4s in NATO. Your president and your secretary of defense have established rules of engagement that don't allow us to fly below 10,000 feet without a SEAD package [that's suppression of enemy air defenses]. My cameras don't work above 5,000 feet. My equivalent of your Joint Chiefs of Staff is a dumb marine, and he says, 'Dutch air force can't take pictures, don't need a Dutch air force.' General, *I* will decide when to risk my men's lives, not your leaders, who don't have the stomach for war." That's probably something that the Americans in the room ought to be thinking about as we work coalition operations.

I was on a coalition operations task force where Bob Scales, who was the commandant of the Army War College, had all of us up to meet with fifty of his foreign students in a two-day

---

[6]President Gerald Ford signed Executive Order 11905, "United States Foreign Intelligence Activities," on Feb. 18, 1976.

exercise up at the College to talk about working together with the United States in coalition and alliance operations. These are side-by-side operations: either the United States leads and they follow, or they lead and the United States follows, as in East Timor. I was really impressed at the candid interchange and still remember the Indian brigadier, who spoke with us about the same subject: "You don't have the stomach for war. It's a national crisis if you lose one individual on the battlefield. In my country, it's glorious for a soldier to die on the battlefield." Some of us weren't that smart about India (although I think I was). He said, "Look at the squalid poverty in my country. To die in glory on a battlefield is a hell of a lot better than being a citizen for most of our people." By the way, I think you need to translate that same situation to the Middle East and understand the struggle that we have in coalition operations when we place this extreme value on human life and if one guy gets killed it's a crisis. Look what we did in Somalia. We ran away.

Oettinger: I may take issue with you. You don't have to go to Asia. Let's stick with the Dutch, the French, and the Brits. An aristocratic officer corps thought nothing of having hundreds of thousands of what they disparagingly called their "cattle" butchered in foolish charges and in the trenches, et cetera.

Rosenberg: We're not disagreeing. The Dutchman said, "We're going to die in battle, and you Americans don't know how to die in battle."

Oettinger: It sounds as though you're siding with the Dutchman.

Rosenberg: No. I was reporting. It's important that we know what other people think of us. When I was a student at the Industrial College of the Armed Forces, George Bush the first was the U.N. [United Nations] ambassador, and he arranged for my class to come up to the U.N. and spend a day with U.N. ambassadors from other countries.

I still remember the butt-chewing we got from the U.N. ambassador from Argentina. He stood up and said, "You Americans are disgusting! You think we must do everything the way you do. We must play football the way you do. Our football is no good. By the way, our football is much better than yours, but unless we play football like you we are a second-class nation. We must play baseball. A lousy sport! We must have two parties. Because we have one party in my country you call us a dictatorship. That's because you are stupid! We come from the kings who took care of their people. By the way, three parties are no good in your country; it must be two. So when will you Americans grow up and realize that it's because you think the rest of the world must be like you that the rest of the world hates you so much?" So maybe I disagree with you a bit, Tony. What I'm trying to do is teach your students what a lot of people out there think about us.

When we got to Afghanistan, we had something we called "morally hardened targets." The air boss was not allowed to shoot. Only CINCCENT [commander in chief, Central Command] approved what we shot at. He had twenty senior people from Muslim countries sitting in the command post down at CENTCOM [Central Command] to whom we were trying to prove we were not at war with the world of Islam, we were only at war with the Taliban and Al Qaeda. For every damn target we had to prove that it was either Al Qaeda or Taliban before we shot a weapon at it. If I ever get to the rest of the briefing I'm going to talk more about that in Kosovo.

After that first trip we did make a lot of dramatic recommendations that made a significant difference, and the next year Bill called us in and said, "Hey, the good news is that this is probably the most valuable DSB task force in the history of the DSB. The bad news is that I'm sending you back over there. This time you're going on the ground in Bosnia, wearing flak jackets, to find out the lessons we should learn to make things better for our next operation." So we went back. Actually, one of the reasons he sent us there was that he wanted to enhance force protection during redeployment. Bill was tired of lessons-learned studies that get put in safes, and then we make the same mistakes again because we don't use these lessons. It turned out that most of the recommendations we made after that second trip were ignored, because the stakes were not very high. When we were on the ground, however, we saw how effective many of these recommendations were. We actually saw national reconnaissance imagery on Russian workstations, which kind of blew the wax out of my ears, but it was as it should have been. By the way, the operations intelligence center was run by a U.S. Army major and twenty crack dog-robber NCOs [noncommissioned officers].

Student: How fast did that national imagery get to the Russians, from the time of the picture down to their station?

Rosenberg: From the time of picture to workstation, it's a matter of the electronic transmission system. The NRO [National Reconnaissance Office] imagery all goes down to a ground station at a classified location, where it gets processed and retransmitted through military communications satellites around the world through a program called DDP—the Defense Dissemination Program. On a selective basis, imagery can get out to a user in a matter of minutes after an image is taken, but there's also a queuing system based on priorities, so sometimes it can take hours.

The important thing is that one of the recommendations we had made on our first trip was to field something that became known as the Bosnia command and control augmentation program. Over the objections of the military, we insisted that this thing called Predator be used operationally during IFOR. Predator had failed its OT&E [operational test and evaluation]. Predator today is still labeled as an unqualified system by the Air Force Operational Test and Evaluation Center at Kirtland. They say it's unsuitable for operational use, which tells you something about the disaster the U.S. Congress has created for OT&E approval of systems. We test systems against useless things called ROCs [required operational capabilities], SNs [statements of need], ORDs [operations requirements documents], and MNs [mission needs], instead of testing them against how well they support operational needs. Nonetheless we said, "You need to field this thing, and you need to pump all kinds of information—digital maps, imagery from all kinds of sources—through commercial wideband direct broadcast satellites down to operational users in the field.

For example (we're talking about IFOR, the thirty-three-coalition partner operation), when the French brigade commander was monitoring the elections in the city of Mostar, he really didn't want to disperse his troops, because they could have been overrun by toughs. The objective was to avoid a fight unless it was necessary. So he kept all of his forces on the edge of town, and he sat in his Humvee [high-mobility multipurpose wheeled vehicle] with an idiot tube. He was getting Predator information, he was getting P-3 video, and he was getting imagery streams from all kinds of sources looking at the polling places, so that if there were riots and disturbances he could send a mass of troops in to quell them.

One of the most marvelous examples of the use of Predator and this direct broadcast link came from the U.S. tank brigade commander. When these guys first went in to IFOR, they went in with guns ready to blaze, because they didn't know whether the guys who had signed up for the peace accords in Dayton would live up to them or not. That was the first phase of the operation. The second phase was to separate the former warring parties, and the third phase was "Put your weapons in storage. You can only take them out when we authorize it for training exercises." The colonel was reporting to us that through Predator he saw the Serbs hiding SAMs [surface-to-air missiles] and tanks out in the forest and in the boondocks, so he confronted this Serbian commander and said, "You're not abiding by the Dayton Peace Accords." "Oh, Colonel, we are! We're scrupulously abiding by them." He pulled out a picture and said, "You're a goddamned liar. See that? There's a robot up there that took that picture, and that robot is up there watching you and me right now. You see those fifty main battle tanks up on that ridge line up there? They're going to blow you to hell in one hour if the robot doesn't see these SAMs being put in those caserns." It was a marvelous marriage of combat power and information.

Student: Sir, has there been any sense of compromise of information or unauthorized use and people getting hold of it? It's one thing if you're working with a relatively unsophisticated enemy, but when you disseminate that kind of imagery through commercial lines it seems to me it would be open to compromise by enemy forces or other intelligence agencies. Obviously, that's what a lot of people worry about.

Rosenberg: What is there to compromise? It's perishable information, isn't it?

Student: Yes, but of source material?

Rosenberg: There's nothing classified about Predator. There's nothing classified about P-3s and their videos. There's nothing classified about LANTIRN [low-altitude navigation and targeting infrared for night] pods on F-16s and A-10s, or TARPs [tactical aerial reconnaissance pods] on F-18s. It's a good issue to raise, because that's the issue that historically my intelligence community (and as a former intelligence officer I can tell you this) has used for years to protect our jobs.

Student: But you're dealing with a more sophisticated enemy, and they have compromised that system. They're now looking at their computers just as you are, and there's a lot of information on mapping the battlespace that it's to your advantage for the other guy not to have.

Rosenberg: That's very true. I just want to be inside his OODA [observe-orient-decide-act] loop. I want to have decision dominance. Technology doesn't belong to the United States. Technology is out there on the world marketplace, and it is those who exploit it better than their adversaries who will win, so I'm not at all concerned.

Now, are there some things we should protect? Yes, there are certain capabilities we should not share. That's why I said that 90 percent of our national intelligence was shared, and 10 percent was not. There are certain things we shouldn't share with anybody. As a matter of fact, classically we in the United States look at warfare as having three levels: the strategic, the operational, and the tactical. A lot of information shouldn't even be given to our warriors at the

operational and tactical levels; it should be kept only at the strategic level. They don't need it to fight at the operational or tactical levels.

Oettinger: I want to underscore again the point you made earlier about how much of this depends on attitude. General Joulwan[7] took great pride in sharing intelligence with the Russians.

Rosenberg: The deal that Joulwan cut and the way he masterminded a compromise were part of how we got the Russians to play on our side. The Russians could easily have ended up on the Serbian side. We were asking them to do something that history has told them they must not do.

Oettinger: It's remarkable in a number of ways. Joulwan tells with great pride that he engineered this. What makes it amusing to me in part is the point about attitude. Some years before that, when Joulwan was a colonel, he was guarding the gate of the then chairman of the Joint Chiefs, General Vessey, and he threw me out of his office. I'd been sent over by one of your successors to ask something of General Vessey in the name of the president and the President's Foreign Intelligence Advisory Board [PFIAB], and Joulwan never even let me through the gate. He threw me out with words like, "We don't need you intelligence wienies messing around with operational stuff!" To see this guy ten years later using intelligence as a tradeoff with great subtlety was a marvelous change in attitude.

Rosenberg: In the briefing we gave Bill Perry after that first trip, one of the things we said was that we're very good at technical intelligence, but if we go to a place like the Balkans, our HUMINT [human intelligence] stinks. If we share our technical intelligence with our coalition partners, they will share their HUMINT with us. Together, then, we can knit a better picture of the battlespace, and the peace enforcement operation will be much more successful. As a matter of fact, that worked very well. When they saw us sharing with them the spigots really did open up a lot.

There was one interesting engagement. We were at Sarajevo and met with the French three-star who wanted to take us to task and told us, "You should go back and see your secretary of defense and tell him what liars you are!" (I love the French.) He said, "You promised you were going to share your high-quality national reconnaissance imagery with us, and all we have is this trash."

Student: Was this before or after the French major was arrested for espionage?

Rosenberg: The point is that we were down at the French brigade three days later, and they had the best NRO imagery we were releasing. (Some of it we weren't.) We said, "We think you ought to go up and tell your three-star he's got a lousy reproduction machine."

Student: Going back to the earlier question about information sharing and the comment that you made about the Russians seeing imagery processed on one of their machines, were they in fact electronically wired into the U.S. system?

---

[7]General George Joulwan, USA, Supreme Allied Commander, Europe, 1995–97.

Rosenberg: The imagery was going through LOCE [Linked Operations Intelligence Capability–Europe]. LOCE was a U.S. system, but it was accepted by NATO as their standard system, and that's how we sent everything. They were operating at a NATO terminal.

By the way, I want to put a bottom line on an earlier comment about the marvelous U.S. Army major, a crack communications guy, and the fantastic crew of sergeants working for him in the operations intelligence center. When we went to the U.S. brigade and saw how terrible their similar operation was—they were starved for information over there—we said, "You know, if he had tried to do that in a U.S. unit this kid would have been court-martialed for violating all the TTPs [tactics, techniques, and procedures] and the other standard things that are inviolate." That's another lecture I'm going to give you: that TTPs don't make any sense. We haven't fought a single war in the last seven years the way we trained for war, and we must untrain ourselves from "evil empire" warfare.

Student: Sir, I'm glad you said what you said about the brigade that was starved for information, because I think I was part of that brigade. I remember many operations where there was a Predator flying overhead, and we couldn't get any data links from it even though we needed them in order to make things happen smoothly.

Student: I was an augmentee at the Bosnia command and control augmentation, and I think your point is well taken. No kidding, we could get near real time to the basement of the Pentagon, but we couldn't get it to the battalions in the hills.

Rosenberg: The guys who had the terminals got it. Guys who didn't have the terminals were out of luck. After all, "You wouldn't give decent communications to warriors, would you?" Disgusting!

Student: You're exactly right. The strategic players had it more often than not. Not only the tactical players, who were certainly engaged, but also the operational players didn't have it.

Rosenberg: Let me fast-forward the clock. We were at war in Kosovo, and the war was just about to end. John Hamre, who was now the deputy SECDEF and had been the comptroller during all the previous operations, said, in effect, "You remember those five idiots who were willing to go over and sacrifice their lives with flak jackets for America? Let's send them back again." So these five foolish, dedicated volunteers—and this time we picked up John Stenbit, who today is the assistant SECDEF for C3I—went over to Kosovo.

We arrived at the end of the war for Operation Noble Anvil. That was the most precise and lowest collateral-damage air campaign in history up until Afghanistan, which is even more precise. Noble Anvil achieved its objectives at the strategic, operational, and tactical levels of war. But what was very interesting is that it started as a two-day coercive campaign to force Milošević to comply with the Rambouillet Accords. If you read the Rambouillet Accords, they asked Milošević to allow us unilaterally to dismember the remains of Yugoslavia, and he wasn't about to do that.

We had done no preparation for anything beyond two days, because, as opposed to Joulwan, Wes Clark[8] tried to keep the NATO alliance intact, and the NATO alliance really didn't want to get involved in a fight. They agreed to a fight. Back in Bosnia, although they were our partners, we were in charge. They essentially were coalition partners, not a NATO alliance, and we ran the war. What happened with Kosovo was that all the NATO allies insisted this was an alliance operation, and every country had veto power over targeting, because they wanted to make sure things didn't go awry. Nobody wanted a land component. We interviewed Wes and everybody up and down the line, and one of the major issues was that there were two European governments that might have fallen if they had supported a land invasion. Suddenly we decided we could win a war with airpower. Crazy!

Student: Are you speaking precisely when you say "No NATO member would have supported a land component," or are you saying that NATO as a whole didn't support it?

Rosenberg: The NATO alliance did not support the use of a land component or force on force in Kosovo.

By the way, an important part of all that is that we went over to the theater, and we interviewed every single commander, from Wes Clark down to the Spanish squadron commander at Aviano and everybody in between, including the Army combat helicopter commander who never got to get into the fight for real, but in fact did have an impact on the operation, interestingly enough. It turned out in our discussions with Wes Clark (and those of you read his book[9] will see that he talks about it fairly candidly) that the biggest opposition he had to the use of a land component came from the U.S. Army. He got no damned support out of his own U.S. Army, because they saw this as a big O&M [operations and maintenance] money eater, and they decided that this could really eat up their budget. As you know, during those years the military machine was really falling apart and unsustainable, so Clark's biggest challenge was fighting a battle with no land component.

Student: Sir, do you mean that opposition came from the Pentagon level, or from the tactical level?

Rosenberg: From the JCS. The guys over in the theater at USAREUR [U.S. Army, Europe] felt denied. They felt violated. They wanted to do their job. As a matter of fact, the 66th Military Intelligence Brigade, assigned to USAREUR in Europe, was not even permitted to participate. They were Army green-suiters, and they're the ones responsible for intelligence preparation of the battlefield and force assessments—red force, blue force, gray force. So JAC [Joint Analysis Center] Molesworth, which was mostly full of other kinds of people, got stuck with that job, and they weren't really qualified to do it.

At any rate, what started as a two-day campaign turned into an open-ended war that we had not trained for, that we had not experimented for, and that we had no campaign plans for, because

---

[8]General Wesley K. Clark, USA, Supreme Allied Commander, Europe, 1997–99.

[9]Wesley K. Clark, *Waging Modern War: Bosnia, Kosovo, and the Future of Combat* (New York: Perseus Book Group, 2001).

our NATO political bosses forbade us to make campaign plans for it. Politically, it was unacceptable for the United States to have an operations plan, so we ended up firing 700 HARMs [high-speed anti-radiation missiles] at their SAMs and did not put a dent into their integrated air defense system, because they didn't use it. They blinked at us: they would turn on, turn off. Milošević was not interested in attrition warfare. He was not interested in fighting a war the way we went into Kosovo to fight—force on force. He hid from us, because his war-winning objectives were simply to avoid getting into a fight. When you have TTPs to use cold war ISR systems in major conflicts, and you get yourself into an asymmetric military operation with an enemy who is not playing by your rules, you stress those kinds of systems beyond their breaking point, which is what we did.

To top all that off, because we could not defeat their integrated air defense systems, General [Michael C.] Short, the air boss, was forced to fly above 15,000 feet to stay out of the kinetic envelope of the SA-6, to avoid the MANPADs [man-portable anti-air devices] and AAA [anti-aircraft artillery]. When you are trying to shoot at a target in the dark of night looking through an IR [infrared] soda straw from 15,000 feet above the ground, you don't see a damn thing and can't hit a damn thing.

So what did we do? When we heard something through a Rivet Joint [RC-135 reconnaissance aircraft] we sent a Predator up there to put eyes on target. There was a flag officer, either at JAC Molesworth or down at Vicenza, who was on an open mike vectoring an AFAC—an airborne forward air controller—to marry up with the Predator. He said, "You see that dirt road?" "Yes, sir." "You see that ridge line?" "Yes, sir." "You see what looks like a vent?" "Yes, sir." "That is the stack from the underground command post." "Ahh, got it!" The pilot lased it, his buddy fired a weapon at it, and that took forty-five minutes, during which time Milošević's forces rounded up a bunch of innocent people, chained them together, and invited the international press to watch NATO butcher civilians.

Remember that I told you that Milošević was inside our information cycle time? We were operating with the Bosnian command and control augmentation program unclassified. He knew exactly where we were taking video. That created all kinds of problems. So did the open mike, but I worried a lot less about the Frenchman who was arrested (we have Americans who do the same thing), because every time a flight of four took off from Aviano there were Serbs sitting at the end of the runway with their cell phones calling home and saying, "In one hour and fifteen minutes they're going to be coming right down the pike." When they shot down the F-117 it was not with a guided weapon, it was with barrage fire, because our NATO partners did not allow us ingress into the battlespace from all avenues. We had to follow international air-traffic routes and rules. With set-piece warfare, the Serbs knew exactly when they could knock us out of the sky.

Student: Sir, from your perspective, how do we solve that problem of restrictive rules of engagement [ROE] when we are in a coalition operation? I was there at the CAOC [combined air operations center] at the time, and General Clark wanted us to shoot tanks using the same methods you were just describing with the Predator. We had the Hunter fly over, and the FAC would have to confirm before we could shoot. I was not able to figure out how we could get through this great restrictive ROE quagmire in the time from sensor to shooter.

Rosenberg: I'm going talk about that philosophically. I had a little problem with General Short and the attitude of us blue-suiters toward our commander, so I need to talk about the policy aspects of who the hell runs a war. At any rate, what you just said is a really serious issue. We invented a term in Kosovo. When my task force came back and briefed the SECDEF, we said, "We now have a new class of targets. We call them 'morally hardened' targets. You can't shoot at a SAM site, because they make sure that it's at a hospital, or in a churchyard, or in a school, and it really changes the act of warfare."

In Afghanistan, we had a confrontation between the air boss, General [Charles F.] Wald, and General Tommy Franks. It was the same kind of stress, because the air boss wanted ROEs that said "Let me go conduct a war and I'll win it," and yet we had the political issue of all these people representing not just Arab nations, but the entire world of Islam, sitting down in the command post at CENTCOM, believing this really was a jihad, and watching us to see if we were going to butcher innocent Muslims, or were really only going to kill bad guys. There was a major confrontation when there was a convoy of pickup trucks and SUVs [sport utility vehicles] going down a mountain pass and the CAOC at Riyadh wanted to kill them. They said, "We know this is Al Qaeda." "No, you actually have to look inside the vehicles." They wanted to blow up the mountain road. No, the ROE didn't allow you to destroy infrastructure, and this was the only road. They finally got permission to fire a JDAM [joint direct attack munition] into the side of the hill to cause a landslide to close the road, because people could then bring in road-clearing equipment and clear it. That stopped the vehicles and allowed them to be inspected, and there were all good guys inside them.

Let me get into this, because this issue is an important one for both the civilians and the military people sitting here in the room. When we went over on that trip to interview all of those commanders and their staffs, we got into the room with my former friend Mike Short. He smashed his fist down on the table and said, "I'll be damned if I'll give you any lessons learned! We should never allow a war to be run in this fashion again." He said that in front of a bunch of his staff officers. I may be in industry and a civilian, but I am still a general officer in the U.S. Air Force until I die (you only retire from active duty; you don't retire). I got up and smashed my fist down on the table, and I said, "That's a bunch of bullshit. I've worked in a dumb Republican White House and I've worked in a dumb Democratic White House, and the probability of this happening again, Mike, is unity. So you owe it to future generations of warriors to learn how to fight under such constraints, because that is the way of modern warfare." We should not cry over the fact that Tommy Franks[10] wouldn't allow us to operate the way we wanted to. We shouldn't cry over the fact that Wes Clark told us, "Yes, I know I told them to go shoot at moving fireplugs" (that's what you kids call useless targets). It turned out that among General Clark's war-winning objectives—and again, read his book, because it tells you this—were keeping the NATO alliance intact and stopping the genocide in Kosovo.

Remember, I told you that we were fighting an asymmetric enemy, and his war-winning objectives were entirely different from ours. He wanted us to get worn down, give up, and walk away. General Clark was convinced that the only way to keep NATO involved was constantly to increase the operations tempo. That was his strategic judgment in consultation with the SECDEF

[10]Gen. Tommy Franks, USA, commander in chief, CENTCOM.

and the president, and that's the way he had to conduct the war. There were a lot of guys who complained that Wes Clark tied up the strategic, operational, and tactical levels of warfare with his insatiable desire to have classified video teleconferences. They said, "God, we should never allow that to happen again." What my task force said is, "That's a dumb view of the use of secure video teleconferences. That capability enables us to collapse the strategic, operational, and tactical levels of warfare into milliseconds, and if exploited properly it would allow us to get inside an enemy's decision cycle very rapidly and win," instead of griping about Wes Clark acting like a battalion commander. Tommy Franks did the same thing when, four hours from target, he'd change the targets that the B-2s were shooting at in Afghanistan. General Franks was in hourly conversations with the SECDEF and the president. So military guys may think they should be unfettered in the way they should prosecute a war, but every one of you raised your hand and said that you serve the political leadership of this country. If you don't like it, resign, rather than gripe about it in uniform.

Oettinger: I happen to agree with you, but I think there's an even more fundamental point to this, which emerged in my mind from looking not only at the record of this seminar over twenty years but also at history and so on. This is an asymmetric problem. Everybody wants to be in control of their subordinates and free of control from their superiors, and that's an age-old axiom. There's no technology that changes that; only the modalities change. MacArthur pretended that his teletype wasn't working, and therefore he wasn't responsive to some of President Truman's orders. Truman won that in the end and fired MacArthur. I traced the history ever since the Korean tree-cutting incident of the relationship between the forces in Korea and CINCPAC [commander in chief, Pacific] and his predecessor in the White House and of the games that were played regarding who would take orders from whom under what circumstances. It is a human relations problem that has to do with superiors and subordinates. The technology is irrelevant. It just changes the tactical means for screwing your superiors and lording it over your subordinates.

Rosenberg: By the way, it's even more difficult in alliance and coalition warfare. In our country, we are actually learning how to allow information to flow simultaneously to get a "common operational picture" (I can't stand that term; there is no such thing) or, rather, a consistent operational picture for all the players to see. We're allowing the information to flow at all levels of forces, and we're depending on ROE as the chain of command. If you go to the German army, or the Brits, most of our partners are still very rigid. The hierarchies of command, control, and information flow are still very much married. That makes it tough.

Oettinger: You don't want the cattle to know anything.

Student: Before you leave that point, General, if you look at those two allies, in particular, and their almost insatiable desire to have a common operational picture—or, at least, our operational picture, which they're willing to accept as the common operational picture—doesn't that fly in the face of the argument? Or do you mean it's flowing from the strategic level to the tactical level?

Rosenberg: No, I meant, "The only thing the major sees is what the colonel wants to let him see, and the only thing the captain sees…." It's the Prussian mentality.

Let me switch quickly to Afghanistan and compare it with Kosovo from a command and control standpoint. Afghanistan, as I said, was even more of the same. There were more morally hardened targets than there were in Kosovo. At the same time we were trying to kill Al Qaeda and Taliban fighters we were trying to prove to the world that we were not trying to kill Afghans, so we had C-17s dropping relief packages of food, but we did a terrible job of that because the packages looked like munitions. Then we dropped leaflets to tell them, "No, it's good food," in a population where 90 percent of the people are illiterate. I'm not saying we're screwed up; I'm just saying that we have to change the way we think about fighting. We have to be a lot more flexible in terms of operations, and I'm going to tell you about a good example of that.

The one thing we were very fortunate about in Afghanistan is that we had continuity. I first met Chuck Wald, who is the air boss in Afghanistan, on my first trip over during the Bosnian war, when he was Colonel Wald. He was the air commander down at Aviano. He had gotten promoted to brigadier general by the time of the IFOR operation, and during Kosovo he had become a two-star general and he was running much of the air operation under Mike Short. So he was the glue of experience. He had learned what Rosie calls "ad hoc kludge." What I'm talking about here is that in this world of C2ISR we need to learn to do something you've read about called "plug and play," because every joint task force is an ad hoc kludge of whatever tanks, ships, and planes a CINC can cobble together. I just told you that Wes Clark didn't do a very good job. He had to beg, borrow, and steal forces from other CINCs, and resource allocations go through the JCS, so he really didn't have what he needed to fight a war. What we need to do is learn to plug together the right C4ISR assets to support that ad hoc kludge of forces. We need to learn how to handle change and become a lot more flexible than we have been.

In Afghanistan we faced even more change. We had no bases. Our good friends the Saudis weren't threatened, so they wouldn't allow us to fly our airplanes out of Saudi Arabia. So what did we do? We had to switch to carrier task force operations as the predominant means of delivering firepower. We flew B-2s forty hours one way from Whiteman Air Force Base in Missouri, and we used B-52s in close air support. We had B-52s loitering over the battlefield.

One vignette of many, many untold famous stories. There was a young tech sergeant named Linehart, a member of the Air Force SOF, who went over there as part of a search-and-rescue [SAR] team. We were sure we were going to get a lot of guys shot down, so we sent in SAR forces. He was dropped out of a helicopter right in the midst of Northern Alliance forces. He made friends with the Northern Alliance force commander, which is what all our kids were supposed to do: let them know we're good guys and we're here to help. He started riding with them on a horse—on a wooden saddle—and this kid had never ridden a horse in his life.

He had all the equipment for SAR: GPS [Global Positioning System] receivers and something called a Viper. That little device kind of came in handy, because after he was out there with the Northern Alliance forces for a couple of days, they rode up to a ridge line and the commander looked out and there were about 300 Taliban in their "armored vehicles"—Land Rovers and SUVs. He said to the sergeant, "Could you get some firepower on them, because in the next several hours or at least the next several days they're going to be a threat to us?" So the sergeant went through his secure SATCOM [satellite communications] and talked to the CAOC, and asked, "Can you give me some firepower?" (This was a satellite war we fought. We didn't shoot any weapons from satellites, but without the satellites we couldn't have done what we did.)

Through the satellite the CAOC talked to a B-52 that had a bunch of sensor-fused weapons on it. Those are the things you've heard about that go *BLAM*, and after they hit a 200-foot-wide by 400-foot-long area ends up looking like a carefully mowed golf course. There was a B-52 up there with about twenty-four of these weapons on it. It came up over the horizon, and the sergeant pointed his Viper at these forces and it recorded their GPS location (not his): their latitude, longitude, and altitude. He uplinked those to the B-52 and the crew fat-fingered them into the weapon, and eighteen minutes after the Northern Alliance commander said, "Would you mind killing those guys?" five of these weapons were laid down just as these vehicles and the troops were on a road. After that a new saying was created: "Space put DAMN in the JDAM!" They were all gone.

This went on constantly during the war. Remember the Arab world version of CNN, Al Jezira, which allowed the other side to be interviewed and talk propaganda every day? There were many occasions where the guys being interviewed were looking up, because they all were talking on radios, and we knew their exact coordinates, so they always wondered when we were going to send them to Allah's heaven. We did on several occasions. People would come out of caves and get on their cell phones at Al Qaeda to communicate with somebody, and not long after they got on their cell phone they weren't there any more.

So it's a whole new form of warfare. The important thing is that's all going to get lost. We went over to Kosovo. All of those very important changes that we told Bill Perry he had to make or he shouldn't put 20,000 kids on the ground five years later were all gone again. We had reverted to seven separate classification systems. The B-2 was in its own compartmented U.S.-only classification system, as was the F-117, which was separate from the B-2 classification system. The first time a B-2 ingressed into the battlespace, opened up its bomb bay doors, and lit up like a 747 when its garbage is out, there was a NATO AWACS [Airborne Warning and Control System] on orbit. It's not configured like a U.S. AWACS; it's a NATO airborne early warning system, and it saw an unknown in the battlespace. Fortunately, we had an unsecure open mike between the NATO AWACS and General Short when they called "Bogey" and were ready to vector fighters to shoot down this unknown, and General Short said, "It's okay; ignore it." My question for you to think about is what kind of confidence and trust-building that creates among members of an alliance and what kind of risk we put on our own forces when we compartment like that.

We did the compartmentation because we knew that our own NATO allies were putting the ATO [air tasking order] in bad guys' hands. But, remember, I told you that at the same time there were Serbs sitting off the end of the runway, passing on all that information anyway independent of the ATO.

Oettinger: Lest you jump to judgment on this, I think this opens up an important set of things. Make notes of what you just heard from General Rosenberg about that B-2 and "Bogey" and the NATO AWACS not configured like ours, and remember it when you read the last book you're assigned this semester, which is Colonel Snook's *Friendly Fire*.[11] It's a very parallel phenomenon:

---

[11]Scott A Snook, *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks over Northern Iraq* (Princeton: Princeton University Press, 2000).

friendly, U.S. on U.S. The question is: How do you avoid such things? What causes them? It's a very deep question that he's raised.

The other one that I quickly want to ride on is what you said a moment ago about "plug and play" and so on. If you haven't read it already, read Graham Allison's *Essence of Decision*.[12] This is an old, recurrent problem, and it's independent of technology. You always have to play with yesterday's toys, because tomorrow's either haven't been invented yet or are so new that nobody knows how to use them. So you're stuck with a dilemma of plug-and-playing a new game with yesterday's toys or using the unknown ones and improvising, and each of them has its own routes for errors. The point I'm trying to drive at you is that if you're prepared to accept that nothing is perfect, life is easier to control, or at least marginally so, than if you have delusions about perfectibility. I've been harping on that since the beginning of the semester.

Rosenberg: I promised I would finish up and not tell old war stories, but there's one that you just drove me to. The first time I stood up in front of the pre-JROC [Joint Requirements Oversight Council], I was the vice chairman of a DSB task force talking about the infusion of modern technology into warfighting. I was making the presentation on my way to briefing the SECDEF. There were all of the one-stars and two-stars and colonels in the room, and I said, "What we want to be able to do is take information off any kind of imaging device and out in the field allow a level-7 NCO or a young lieutenant to download that imagery right into his digital map and update it to give a tailored product to the people he's supporting to fight the war with the current view of the battlespace." In the back of the room a colonel stood up and said, "Mr. Rosenberg, I've heard enough. The DSB doesn't know what the hell it's talking about. You can't expect people to do that. That's just nonsense."

When I ran the DMA, that colonel was a lieutenant colonel commanding an engineering topographic battalion over in USAREUR. He was what I call a geomorph—a professional little old mapmaker who took my maps from DMA and did go/no go maps for main battle tanks over in the European theater. I looked at him and said, "You know, Colonel, until you opened your mouth I thought there was only one senile person in the room. Now I know there are at least two of us." I looked at all the admirals and generals and I said, "I suggest you all leave the briefing if you agree with him, because you are not salvageable. But by the way, when you leave, go by the Pentagon City arcade and watch the thirteen-year-olds playing wargames on the machines over there faster than the speed of light, doing exactly what I'm talking about. When you get home tonight and think your teenage daughter is doing her homework, peek in her door and watch her cruising cyberspace on AmericaOnline doing everything I'm talking about, while you old goats, who are afraid of information technology, refuse to write the POM [program objective memorandum] and budget what our young warriors need in their hands to do their jobs." Remember, I opened this presentation by saying that, despite the trash we give them, the young kids cobble it together and they make it work and they win wars.

---

[12]Graham T. Allison and Philip Zelikow, *The Essence of Decision: Explaining the Cuban Missile Crisis*, 2nd ed. (Reading, Mass.: Longman, 1999).

Let me wrap up so we've got a couple of minutes at least for you to shoot at me. I'll leave the paper I've been talking from, because it goes into a lot of this stuff in more detail,[13] and I'll send you a quiz after you've read it.

These are the challenges that we found in our visits. Complicated coalition and alliance processes are a way of life, and we have to get used to them. There's no such thing as a U.S. JTF [joint task force] alone. Alliances and coalitions are key enablers that require consensus. Sometimes we lead, sometimes we follow.

I've already talked a lot about untraining ourselves from "evil empire" warfare. Do you think anybody trained for what we did in Afghanistan, or for what that sergeant did? As I said, he went over there as a SAR guy, not as a forward air controller, so don't tell me youngsters can't do the job.

Our current practices in the DOD, namely OPSEC [operational security] and COMSEC [communications security], are not compatible with the real world. When you overclassify things—these seven separate classification systems—the kids out there who are in the fight (and those of you who were over there know what I'm talking about) throw up their hands and say, "This is nonsense!" and share stuff with their partners anyway. The problem is that when you have a system you can't believe in, you will end up sharing stuff you shouldn't share. We really need a system we can depend on, because when you end up in that kind of environment, you end up busting OPSEC, too, to get around things. If we got ourselves a realistic security paradigm of going from cold war system-high to modern warfare system-low, where we only protect the ultra-secret crown jewels at the compartmented level and everything else we share among ourselves and our coalition partners, we would have a lot fewer accidents and a lot less loss of life.

Oettinger: Rosie, am I nutty? I would put that in a somewhat different way, and I want to see if you agree or disagree. What I've preached here in earlier sessions and in stuff they've read is the notion that OPSEC and operational effectiveness are tradeoffs, in that you've got to make judgments. Do you have any words of wisdom on how one will make those judgments, so that regardless of what level you're at—strategic, operational, or tactical—you can make a sensible judgment?

Rosenberg: What I'm going to give you is a DSB recommendation, which I believe is the right way to try to evolve this. That is: Security should be controlled in a risk management sense, like a rheostat. If I'm on the offense, and inside my enemy's decision cycle and really on the go, I can loosen up that rheostat, because a lot of what we're talking about is very perishable information anyway. It's not a matter of sources and methods, it's a matter of whether the enemy can use this information that I'm allowing to flow in the open. If he's rapidly backing off on defense, no, he can't. On the other hand, if you're in a stalemate situation, you really have to tighten up the rheostat. We've got to get away from absolute rules of what fits in one compartment and what fits into another, to the point where the battle commander is able to manage risk.

That's true for blue force information as well as red force information. One of our most serious problems in IFOR was that the land component commander was a Brit. His background

[13] See footnote 2.

was Northern Ireland terrorism, and blue force information meant dead British soldiers. So he absolutely prohibited the ground order of battle to be published with blue force information in it. Remember, this was urban warfare. Peace enforcement is urban warfare. We were trying to avoid a fight. Here were the Belgiques being surrounded by a bunch of toughs and the Belgian commander wanted to call in a flight of four from NATO to shake the mighty fist of NATO, but NATO didn't know where the hell they were, because the British commander didn't allow the information out. Hey, man, it isn't just the White House that has the problem! Our coalition partners have it, too. Do I have a solution? No. What I'm telling you is that we have to learn to live with that instead of saying "I don't want to get involved." We're going to get involved and have to live with it.

Student: Can I take you back to your notion of the rheostat and the risk? I'd like to couple that with your idea of flexibility and enhanced kludgeability in building up war plans. If we look at intelligence and try to build a reasonable construct plan for enhanceability and flexibility, something to have on the shelf, how does that couple with this rheostat of intelligence and the preparation of the battlefield? I'm talking U.S.-only here. How do we back off on OPSEC and get releasability for data to build that plug-and-play tool?

Rosenberg: I'd say build it and they will come. There will be cases where the restrictions don't allow you to do that. Then there will be cases where the SECDEF and the DCI know there's enough at stake. All the rules were different in Afghanistan, because we had a real enemy. With 20,000 kids on the ground we really meant it, because we didn't want to put them at risk. In Kosovo we reverted, because nothing much was at stake. Now, somebody kills a bunch of Americans in the World Trade Center and we're at war. The CIA can't stand the release of national intelligence to support those tactical folks, but, suddenly, when you've got a CIA kid on the ground in Afghanistan, it's national intelligence, so policy barriers fall.

Oettinger: It's easy to sneer. You'll hear from some folks on the other side of that argument. In fact, you could read Jim Simon's "Crucified on a Cross of Goldwater–Nichols" on our Web site.[14] It's guys like him that Simon is talking about.

Rosenberg: He and I totally disagree.

I want to close quickly with this: ISR is currently not connected to command and control. We've got a problem here. We've got all these national intelligence collection assets and theater assets and tactical assets, and they're not connected. They're all out there doing their own thing, because they all grew up in the cold war environment. The NSA [National Security Agency] thinks they own Rivet Joint. CIA thinks they own NRO imagery satellites. (There's a little bit of sneer in all this, but a little bit of reality, too.) None of them is tied together.

Let me give you an example. During IFOR, all of the leaders wanted most of all to search for, locate, and track high-level war criminals. They didn't want to capture them because we didn't want to start a war, but they wanted to keep track of them. We have a marvelous little

---

[14]James M. Simon, "Crucified on a Cross of Goldwater–Nichols," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2001* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-01-3, July 2001), [On-line]. URL: http://www.pirp.harvard.edu//pubs_pdf/simon\simon-i01-3.pdf

collection toy called Guardrail. It's really neat. These guys were moving between midnight and two a.m. with push-to-talk radios or low-flying helicopters, and Guardrail is just the ticket to collect SIGINT against them. We were tasking Guardrail between noon and two p.m., not midnight and two a.m., and we asked the joint ISR cell, "Why the hell aren't you tasking Guardrail?" "That's a corps commander's asset. It belongs to General Nash."[15] "Well, dammit, General Nash is the guy who wants the problem solved! If he knew that his little toy, in conjunction with Rivet Joint and U-2s and national reconnaissance satellites, could solve this problem, I'll bet you he'd be happy to share it with you."

Guess what? In Kosovo, the joint targeting cell had to operate Hunter. There was no land component. Hunter is a corps commander's asset, and we didn't have a corps commander, and we weren't trained to operate Hunter. So the little lecture that comes with this is that national, theater, coalition, commercial, and organic reconnaissance and surveillance are done by totally separate processes that don't leverage one another for battlespace dominance, and important sources of information are not being used because they are not part of "classic" ISR.

I looked at freeze-frame video from a Navy F-18 TARP that showed a bridge in the water—down. We sent aircrews against that bridge three times after it was down. The reason? We were only using national reconnaissance imagery for BDA [battle damage assessment]. Stupid? No, it wasn't stupid. It was the only thing we really had TTPs for and processes that really worked. There was no way to take that freeze-frame video, stuff it into NIPRNet [Nonsecure Internet Protocol Router Network], have it go through NIPRNet and up through SIPRNet [Secure Internet Protocol Router Network] into Intelink, come out on a BDA analyst's desk, and say, "You got mail! Use it!" That's how far behind we are in understanding how to use the Web.

More important, we're not creating knowledge in the battlespace either. When an underground command-post communications signal goes from presence of signal to no signal at the same time, we know in the ATO we had a TOT [time on target] that was supposed to have a strike, and if in the computer you marry "Here's when the weapon was going to hit that underground command post and the communications signals went to zero," the probability of kill might not be 100 percent but it sure as hell is better than zero. But still we send crews in over and over again to keep restriking those things, because we don't have modern information management, broadcast management, and network management capabilities.

Student: Doesn't that fly in the face of this notion of effects-based targeting?

Rosenberg: No, it totally supports it. What I'm talking about is providing capabilities to create effects on the battlefield. We have major shortfalls in modern information management, broadcast management, and network management. We need to provide a common geospatial reference for all military information. Critically needed information support to lower echelon forces remains a very weak link. Bandwidth on demand is something we do in the commercial world all the time. Why the hell can't we do it in the military world? Would you tell me? Is it those old guys like Rosie who are afraid of computers and don't understand modern information technology who are making the POM and budget decisions?

---

[15]Major General William Nash, USA, commander of Task Force Eagle, charged with implementing the Dayton Accords.

At any rate, when you raise the subject of effects, there are all kinds of information sources that we aren't using, because we aren't doing what the modern commercial world is doing, and that is Web-enabling ourselves. There's hand-held video; there are all kinds of information. I work on an advisory board for General Clapper, the director of the National Imaging and Mapping Agency [NIMA], and he's got a guy named Bran Ferren, who used to be with Disney. What we need is the mother of all databases—a virtual database—instead of serial information. It's not beyond the realm of the possible. If I were an analyst, it wouldn't matter if I were at a JIC [Joint Intelligence Center] or a JAC or aboard a command and control ship. No matter where I was, I would have a home page that says, "I'm responsible for providing situational awareness, threat assessment, targeting, and BDA for this hunk of latitude-longitude coordinates," and my little "knowbots" would go out through digit heaven and find relevant stuff that people have put there.

You may ask, "What about the latency?" I just went to a lecture on the workplace by John Gray, the guy who wrote *Men Are from Mars, Women Are from Venus*, and he said that women have four segments in their brain that all operate at the same time and we Neanderthal men process serially. What we need to do is multitask as women do. By the way, he also said that women have a superhighway between the thinking and feeling parts of the brain and the speaking part. That's what the Web does, and we need to take advantage of that. My daughter tells me that if I speak properly, She (God) will be kind to me.

Student: In the current war against Afghanistan, NIMA is exploiting a lot of commercial imagery, and although the quality is not good enough for targeting, it's sufficient for below-one-meter operations. I was wondering if exploitation of commercial imagery could be one solution for the tension between security of information and the need to share.

Rosenberg: Yes, there's a lot of good use for commercial imagery in making digital geospatial information systems, which are kind of the modern version of maps. I hope we're going to get away from maps some day and go to virtual reality geospatial information. Certainly, commercial imagery satisfies a lot of those needs, and it is just as accurate as national intelligence information because the commercial imagery is overlaid on a database that is based on the good stuff. So it provides a lot of what we need for targeting, for terrain analysis, and for mission planning.

We do have a problem in our country, however. The government wants to sponsor a strong, space-based commercial industry to become the international leader, and yet we are schizophrenic about that because we want to have shutter control when we're in a war. It created very serious problems for the commercial imagery providers when all of their customers worldwide were denied the imagery they paid for during this combat operation in Afghanistan. We can't have our cake and eat it. We can't be the commercial world leaders in space-based imagery and yet still want to prevent other people from having it. It's the same issue that was brought up earlier.

Student: What about GPS?

Rosenberg: I hear this all the time: "Rosenberg, you're a traitor to the nation wanting to let everybody use GPS!" Rosie's standard answer to that is that GPS is worthless to our enemies unless they can exploit it as well as we can. The important thing is how you can take that information and use it to kill somebody before he can kill you. We're a hell of a lot better at that

than most other people are in terms of exploitation of information technology, in spite of the old goats like me who are afraid of it. Technology does not belong to the United States. It belongs to the world. It's those who exploit it better and faster than their adversaries who will dominate in conflict.

Student: Currently there are two proposals for reorganizing the NRO. The one from the Space Commission would integrate it better with the Air Force, and the other, from the PFIAB, would actually give all of NIMA, NSA, and NRO to the CIA instead. I know it's partly a turf issue, but which one would you favor?

Rosenberg: It's not a turf battle. It's all men and women of goodwill. They are all dedicated citizens who are convinced that their solution is the right one. I won't take sides.

I worked in the White House (actually, Tony helped me as a NSC advisor) in the days when there was much strife over what is national and what is tactical. Let me just say that when there are 20,000 U.S. kids on the ground in a war zone, that's not tactical intelligence. The president of the United States considers their safety national intelligence. It's different strokes for different folks at different times.

I think that Scowcroft and the PFIAB are rightly concerned that we have lost our way in the national intelligence community. The very fact that there are many people in the national intelligence community who do not believe that 9/11 was an intelligence failure tells you we are sick. I have friends and colleagues who are national intelligence officers who insist that was not an intelligence failure. I insist it was—of the worst order. I'm not blaming the CIA or the DCI or anyone else for that. I blame us, the American people, for that intelligence failure, because we have dismantled our national security apparatus over the past several years. What the Scowcroft group is recommending for the NRO is their fix to get more of a focus on national intelligence problems. I don't take issue with what they recommend, nor do I take issue with the other side of it, because the Afghanistan war is being run on a daily basis with direct involvement of President Bush and Vice President Cheney, and there's a lot of tactical intelligence supporting military warfighters. We need to forget this "what's national and what's military." If, instead, we go to what I have been preaching to you about, which is a Web-enabled world of information sharing in real time, where people who have a need to get it get it right now, we would far improve support to both national policymakers and to the poor kid out on the battlefield who's got a gun pointed at him.

Oettinger: I've got to get you to an airport. Sir, thank you very much, and here's a small token of our great appreciation.

Appendix 1

2-25-02

IMPROVED APPLICATION OF INFORMATION TO THE BATTLEFIELD
REVISITED**

REMARKS BY
MAJOR GENERAL ROBERT A. ROSENBERG, USAF (RET.)
Executive Vice President and General Manager, SAIC Washington Operations

- ♦ What we have learned from the Balkans—seven years later with reinforcement from the Noble Anvil (Kosovo/FRY) campaign, and similar experiences in the recent Afghan campaign
  - Focusing on C4ISR
  - My comments are applicable to other military operations, including MRCs
- The good news is that we made information flow to wings, carrier battle groups, and divisions in the Bosnia, Kosovo/FRY and Afghan theatres much more robust—so we know it can work well anywhere else and could be done worldwide
- We found that American military, civilian, and contractor talent to get the near-impossible done when called upon by our nation still flourishes and excels with innovation and initiative…in spite of limited resources we gave them, little time to plan or train, and political constraints that sometimes make it even tougher to succeed.
- Three weeks after the O'Grady shoot-down in 1995 Secretary Perry asked a small group of us to go to the European theatre and return with dramatic recommendations to make it a much safer place to put 20,000 US troops on the ground in Bosnia:
  - It should be noted from the history of the German occupation in WWII that they lost one in seven "peacekeepers" to guerrilla warfare there—peace enforcement is a dangerous military mission
  - At the time the SecDef called us in, we were flying 40 sorties/day to keep 21 Bosnia-Serb airplanes on the ground—and were unsuccessful
  - They had information dominance of the battlespace
  - They were inside our information cycle time
- We made several recommendations to the SecDef, DCI, and Vice Chairman after observing the Bosnia bombing campaign in real time from carriers and command centers to fighter squadrons ashore and SOF forces.
- Resulted in joint DOD/CIA implementation of many recommendations
- These problems were dramatically improved upon before the IFOR peace enforcement mission was on the ground in 1996
- In a subsequent trip back to the theatre in the summer of '96, including on the ground in Bosnia, we visited 17 units in 14 days—land, naval, air; French, Brits, Russians, US—down to the brigade and battalion level, wings, command and control ships and carrier battle groups

The SecDef asked us to recommend further C4ISR improvements to support peaceful national elections in B-H, to enhance force protection during re-deployment and lessons to apply to other theatres and contingencies. He was tired of lessons-learned studies that get put in safes and then we make the same mistakes again because we don't use these lessons.

- Once again the group made several recommendations.

- In the summer of 1999, many of the same team were asked one more time by the DepSecDef and ASDC3I to return to the Balkans on yet another Task Force. This one, chartered in early summer, was asked to review C4ISR operations in the recently completed operation in Kosovo and the FRY and to make recommendations on both near- and longer-term technical and operational improvements to capabilities currently providing support to NATO operations in the Balkans, as well as other future military operations worldwide

Noble Anvil was:

- The most precise and lowest collateral damage air campaign in history
- It achieved its objectives at the
    - Strategic,
    - Operational, and
    - Tactical

      Levels of War
    - What started as a two-day coercive campaign became open ended
    - We fired 700 HARMs at their SAMs
    - Their surface-to-air threat forced us to stay high, facing hiding enemy
        - "Morally hardened" targets became a reality—we couldn't attack some targets because of collateral damage potential
        - It was often mandatory to have eyes on target (BVR wasn't allowed)
        - Coupled with alliance consensus
            - Targeting
            - ROEs
- Zero air crews were lost in 78 days, round-the-clock, 38,000 combat sorties
- This was the largest NATO combat operation in history
- 13 of 19 allies provided aircraft; 300 + allied aircraft flew over 15,000 sorties
- We had terrible weather and terrain – can't hit what you can't see with laser & EO
- We were heavily dependent on GPS guided weapons
- There was a need for extreme precision to minimize collateral damage
- And we were in an urban warfare campaign
- With no land component to shape the battlespace
- Fighting an asymmetric enemy
    - No force on force
    - Different war winning objectives—his objective was to wear us down

As part of the review, the Task Force met with commanders and staffs at all levels of command in the European theatre engaged in the operation, from strategic, through operational, to tactical; from SACEUR General Wes Clark down to individual air crew members and peace enforcers on the ground today

- We even flew over Kosovo in armed combat helicopters with MEAT Team doing ground truth for BDA

- We found challenges in our three visits to the theatre that are pervasive for most military operations that we have been and will be engaged in since the fall of the Berlin Wall—as well as future major conflicts—not just the Balkans. These include:
    - Complicated coalition/alliance processes *are* a way of life
    - We must get used to this
    - No AEF or JTF alone
    - Alliances and coalitions are key enablers that often require consensus
    - Sometimes we lead, sometimes we follow, as in East Timor
    - We must untrain ourselves from Evil Empire warfare
    - We haven't fought a single Balkan campaign the way we trained
    - OPSEC/COMSEC are not compatible with the real world
    - Cold War hardware and TTPs for Fulda Gap warfare in an untrained environment with excessive security barriers lead to busted OPSEC
    - Nonessential security barriers prevent rapid or useful information flow
    - The need for more information sharing among coalition partners
    - Inadequate exploitation of existing military and commercial bandwidth
    - Dynamic reconfigurability of C4ISR: we don't have it—and we need it
    - ISR not connected to C2
    - National theatre, coalition, and organic recce/surveillance done by totally separate processes that don't leverage each other for battlespace dominance—as well as important sources of information not being used because they are not part of "classic" ISR
    - Major modern information management, broadcast management, and network management shortfalls
    - Providing a common time-tagged geospatial reference for *all* military information; without it we drop billions of bits on the floor and can't find or use them again
    - Critically needed information support to lower echelon forces remains a very weak link

Focusing on a few**:**

- SECURITY BARRIERS: On our first Task Force visit in 1995, we found security barriers preventing warriors from getting information they needed in a timely fashion—all or not at all—creating sneaker nets and fat-finger inputs between US sources and coalition C2 systems that seriously impacted our ops cycle time

  We found a critical need to share and integrate information among coalition partners—in fact, operating from a separate sheet of music increases risks to US forces.

    - In many ways our coalition partners are better at HUMINT than we—it's usually their natural turf—while we are better at technical collection
    - In the B-H theatre they were taking advantage of information sharing better than we were in many cases because our C4I systems weren't able to receive coalition information electronically—that continues today—both because of flawed US security policy and lack of commitment to use coalition information.

  We recommended a new security paradigm to go from Cold War Systems High to Modern Warfare Systems Low. During IFOR, 90% of our national intelligence flowed from point of

origin at SECRET IFOR to dramatically speed up the OODA loop—this would be an important improvement to do today in Korea, as well as for other coalition operations and theatres—but in Noble Anvil, we retrogressed to seven separate security systems, partly because of inadequate OPSEC/COMSEC, finding ourselves bogged down again.

We must redefine the Cold War security classification paradigm which so badly slows down the OODA loop with so many separate security systems—resulting in islands of computers connected by miles of sneaker nets, fat fingers, and air gaps—to allow the flow of information electronically across the many stovepiped network-centric systems and shared with our coalition partners—protecting multiple levels of security through modern available software solutions—rather than continue to pursue outdated Cold War hardware-oriented approaches to MLS. Only the "Ultra Secrets" should be behind such barriers—and not shared.

- C4—NOT CONNECTED TO ISR: The only place C4 is integrated with ISR is in the JCS JROC JWCA
  - We stressed ISR assets beyond their breaking point by using Cold War developed systems with Cold War TTPs that we had to modify on the run in a brave new world of military operations against an enemy who was either hiding or moving faster than our OODA loop, creating zero collateral damage restrictions, requiring eyes on target before weapons release
  - We need a dramatic paradigm shift to dynamically integrate recce/surveillance assets into the ops tempo of combat—as essential to the success of joint and coalition ops—not separate ISR integration!
  - We must make major improvements in operational integration of C4ISR directly coupled to shooters by fielding a distributed "virtual" armed recce/strike/re-strike capability—starting with integration of theatre assets such as JSTARS, RIVET JOINT, U2s, ABCCC and Predator, and extending later to national, organic, and coalition assets. We must include commercial and international sources, targeting pods, gun cameras, and other "non-classical" ISR assets in this new paradigm. We must change ISR from looking at targets to killing them

The need for extremely precise and rapid battlespace knowledge of the target and the target environment to avoid collateral damage requires us to change the way we've always done it.

  - We must develop the doctrine and implement the TTPs for recce-strike and adaptive and dynamic effects-based targeting and retargeting driving cross-cueing of sensors, fusion of sensor data, and near real time re-tasking of sensors to rapidly verify BDA and "Eyes on Target" when needed
  - And we must provide better tools for integrated collection and production management of multiple information sources
  - Real experiments, then exercises are needed to practice C2ISR integration
  - At least some systems will develop integrated process
  - Even though not integrated, relationships with other systems will be developed
  - When real crises begin, integrated elements will be deployed and will have knowledge of who or what the non-integrated elements are and how to interface with them in an ad hoc manner
- C4ISR RECONFIGURABILITY NEEDED: Modern world military operations demand dynamic reconfigurability of C4ISR

  - Each JTF is an ad hoc kludge of the tanks, ships, planes, and warriors that a CINC can muster to do a particular job
  - That means forget "Train the way we fight"—we need a new training paradigm—change is the baseline
  - In the world of C4ISR, we need to be able to hook together the right hardware, software, information databases, sensors, and comms to support each—tailored to their needs
  - I call that enhanced kludgeability
  - And we can only do that if we catch up with plumbers, carpenters, and electricians who all have signed up to commercial standards!
  - That's "plug-and-play"
- INFORMATION MANAGEMENT NEEDED: Operations are plagued by inadequate information management concepts, tools, and systems that limit access to information located somewhere else in the system. There are:
  - No quick ways to search for available information for specific objectives
  - Database incompatibilities that aggravate search process
  - Multiple source video archiving not possible
  - Information still not available in a common geospatial reference system
  - HUMINT, IMINT, COMINT, ELINT, UAV video, and other sensor data that could support timely targeting, BDA, and other time-critical decisions aren't provided on a "you've got mail" basis, so we send warriors unnecessarily in harm's way against already destroyed targets!
  - Information and intelligence from lower echelons do not flow easily up the chain of command
  - Greater information support at lower echelons is still lacking at wing, squadron, brigade, and battalion. They still:
  - Have limited communications and information system support
  - Don't know what information is available
  - Lack information tools
  - Lack analysis capability to use information made available
  - Doctrine, tactics, training, and procedures do not cover flexibility needs, without ad hoc additions, in the dramatically changing information environment of near-simultaneous availability of data/information at the strategic, operational, and tactical levels
- NETWORK MANAGEMENT NEEDED: While there are lots of "network-centric systems" like "Global Grid," Intelink, SIPRNET, NIPRNET, IT21, etc., proliferating data simultaneously at strategic operational and tactical levels, and *each stovepiped*, there are inadequate network management concepts, tools, and systems that allow access to and transfer from one network-centric system to another
  - We must link them together, using modern commercial multiple levels of security systems to control who can get it.
  - Only Intelink should be isolated and it should only carry the crown jewels—today it carries everything
- BANDWIDTH ON DEMAND ESSENTIAL: Fundamental to command and control is the ability for participants to communicate seamlessly and reliably with other appropriate participants. This requires an operational system of military and commercial comm systems that provides robust reachback and operational control of network management systems that ensure global connectivity, reliability, and performance providing adequate bandwidth on

demand. What we need—prioritized and managed access to all available links—we do not have, and fiber doesn't get us to the cockpit or the turret!

- INFORMATION SERVICES—WE NEED THEM: There is no current operations architecture that enables real time production, integration, and management of national theatre, organic, commercial, coalition, and alliance information resources, including tasking and information processing, production, and distribution that facilitates getting the Right Knowledge to the Right Users at the Right Time. There is a critical need to operationally provide a dynamic information management system based on the DII COE that makes transparent to users at the strategic, operational, and tactical levels of military operations the storage, search, and retrieval of information—given the potential connectivity, the access to, and the management of huge varieties of data and information that must be controlled

SO WHAT!

- If we do this for modern world military operations, we will have the right C4ISR architecture for major conflicts and transformation as well
- Finally, managing all that information that technology is spilling on the battlefield will be critical to the success of:
  - Joint Vision 2010 and JV 2020
  - Dominance concepts that come from effective combination of combat and information power
  - We must get critically needed information support to lower echelon forces. SINCGARS radios on HUMVs are not what warriors doing nation-building and many other military operations need—the last dirt mile is still broken
- We need major initiatives to infuse technology and take advantage of commercial web technology tools to manage all the data we are dumping on the warrior who, particularly at lower echelons, is still starved for useful information
- We must institutionalize the follow-on use through integration into "the system" of innovative initiatives that occurred in Noble Anvil, other military operations, and ACTDs—rather than just reporting them in lessons-learned studies that don't get implemented
- We need to operationalize new information concepts of "smart push–smart pull" available at all echelons with modern web technology tools—enhanced by unique military value-added applications
- We need direct broadcast, commercial wideband, and fiber coupled with smart broadcast, information, and network management with anchor desks as proactive providers of products––otherwise we will continue to saturate warriors with data and starve them for useful information!

***This paper is a further update of a paper prepared in later 1997 after the original Task Force visit to the Balkans in 1995 and 1996. It was prepared to reflect added observations from the Task Force visit to the Balkans in the summer of 1999 following the Noble Anvil military campaign—and notes similar experiences in the recent Afghan campaign.*

Appendix 2

IMPROVED APPLICATION
OF INFORMATION
TO THE BATTLEFIELD

Robert A. Rosenberg
Executive Vice President

SAIC®
An Employee-Owned Company

- We made information flow to wings, carrier battle groups, divisions and brigades in the Bosnia, Kosovo/FRY, and Afghanistan theatres much more robust—so we know it can work well anywhere else and could be done worldwide.
- American military, civilian, and contractor talent to get the near impossible done when called upon by our nation still flourishes and excels with innovation and initiative.

2

- Challenges found that are pervasive for most military operations
  - Complicated coalition/alliance processes are a way of life
  - We must untrain ourselves from Evil Empire warfare
  - OPSEC/COMSEC not compatible with the real world
  - Nonessential security barriers that prevent rapid or useful information flow

3

- The need for more information sharing among coalition partners
- Inadequate exploitation of existing military and commercial bandwidth
- Dynamic reconfigurabilitiy of C4ISR—we don't have it—we need it

4

– ISR not connected to C2

National theater, coalition, commercial and organic recce/surveillance done by totally separate processes that don't leverage each other for battlespace dominance--as well as important sources of information not being used because they are not part of "classic" ISR

5

– Major modern information management, broadcast management, and network management shortfalls
– Providing a common geospatial reference for all military information
– Critically needed information support to lower echelon forces remains a very weak link

6

Focusing on a few solutions...

- Security Barriers
- C4--Not Connected to ISR
- C4ISR Reconfigurabilitiy Needed
- Information Management Needed
- Network Management Needed
- Bandwidth on Demand Essential
- Information Services…We Need Them

7

So What…

- If we do this for modern world military operations we will have the right C4ISR architecture for major conflicts and transformation as well
- Finally, managing all that information that technology is spilling on the battlefield will be critical to the success of:
  - Joint Vision 2010 and JV 2020
  - Dominance concepts that come from effective combination of combat and information power

8

- We need major initiatives to infuse technology and take advantage of commercial Web technology tools to manage all the data we are dumping on the warrior who, particularly at lower echelons, is still starved for useful information.

9

- We need to operationalize new information concepts of "smart push-smart pull" available at all echelons with modern IT tools—enhanced by unique military value-added applications.
- We must institutionalize the follow-on use through integration into "the system" of innovative initiatives that occurred in Noble Anvil, other military operations, and ACTDs—rather than just reporting them in lessons-learned studies that don't get implemented

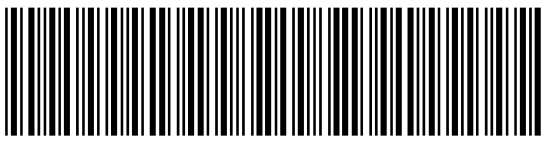
10

Acronyms

AAA	antiaircraft artillery
ATO	air tasking order
AWACS	Airborne Warning and Control System
BDA	battle damage assessment
C2ISR	command, control, intelligence, surveillance, and reconnaissance
C3I	command, control, communications, and intelligence
C4ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CAOC	combined air operations center
CENTCOM	U.S. Central Command
CIA	Central Intelligence Agency
CINCCENT	commander in chief, Central Command
CINCPAC	commander in chief, Pacific Command
COMSEC	communications security
DCI	director of central intelligence
DIA	Defense Intelligence Agency
DMA	Defense Mapping Agency
DOD	Department of Defense
DSB	Defense Science Board
DSCS	Defense Satellite Communication System
FAC	forward air controller
FRY	Federal Republic of Yugoslavia
GPS	Global Positioning System
HUMINT	human intelligence
IFOR	Implementation Force [Bosnia]
IR	infrared
ISR	intelligence, surveillance, and reconnaissance
JAC	joint analysis center
JCS	Joint Chiefs of Staff
JDAM	joint direct attack munition
LOCE	Linked Operations Intelligence Capability—Europe
MRC	major regional conflict

NATO	North Atlantic Treaty Organization
NCO	noncommissioned officer
NIIRS	National Imagery Intelligence Rating Scale
NIMA	National Imagery and Mapping Agency
NIPRNet	Nonsecure Internet Protocol Router Network
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	National Security Council
O&M	operations and maintenance
OPSEC	operational security
OT&E	operational test and evaluation
PFIAB	President's Foreign Intelligence Advisory Board
POM	program objective memorandum
ROE	rules of engagement
SAM	surface-to-air missile
SAR	search and rescue
SECDEF	secretary of defense
SIGINT	signals intelligence
SIPRNet	Secure Internet Protocol Router Network
SOF	special operations forces
SUV	sport utility vehicle
TARP	tactical aerial reconnaissance pod
TOT	time on target
TTP	tactics, techniques, and procedures
U.N.	United Nations
USA	U.S. Army
USAF	U.S. Air Force
USAREUR	U.S. Army, Europe
USN	U.S. Navy

INCSEMINAR2002



ISBN187971681X