

INCIDENTAL PAPER

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

21st Century National Security Challenge
David S. Alberts

Guest Presentations, Spring 1997

Philip B. Heymann; Kenneth Allard; Denis Clift; Douglas D.
Bucholz; Arnold E. Donahue; Charles A. Briggs; Anita K. Jones;
David S. Alberts; Gregory J. Rattray

April 1998

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 © 1998 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 1-879716-47-X I-98-2

21st Century National Security Challenges

David S. Alberts

Dr. David S. Alberts is currently Director of Advanced Concepts, Technologies, and Information Strategies at the Institute for National Strategic Studies, National Defense University. This assignment includes responsibility for the School of Information Warfare and Strategy and the Center for Advanced Concepts and Technology. He also serves as the executive agent for the DOD Command and Control Research Program. Dr. Alberts has over 25 years of experience with all phases of the design, development, and evaluation of innovative, state-of-the-art computer systems, including expert, investigative, intelligence, information, and command and control systems. His government career has included policy and management responsibility for the introduction of technology into operational environments, functional analysis including process reengineering, and system acquisition and design. Dr. Alberts has also worked extensively to evaluate the contributions of both government and industry computer systems to the organizations and missions they support. He frequently contributes to government task forces and workshops on systems acquisition and evaluation. His academic career has included professorial rank posts at New York University and the City University of New York. He received a B.B.A. in Statistics from the City College of New York, and an M.S. and Ph.D. in Operations Research from the University of Pennsylvania.

Oettinger: As usual, I need not go into details because you've read Dr. Alberts' biography. I will just say that it's a great pleasure to have him here because of my long-standing personal collaboration with him and also with his institution. His willingness to come out of his way on shorter notice than usual is greatly appreciated. With that, I turn the floor over to him. He has agreed to be interruptible with questions as he goes along.

Alberts: Thank you. Tony asked me to start off by just telling you what I do for a living. I run what's known as the Advanced Concepts, Technologies, and Information Strategies bunch over at the National Defense University. That includes the School of Information Warfare and Strategy, which basically has now evolved into a majors program for candidates who go to the National War College (NWC) or the Industrial College of the Armed Forces (ICAF), as well as a lot of outreach programs for senior DOD civilians and military officers. We also have a very large research program, by university standards, which is

funded by OSD (Office of the Secretary of Defense). We undertake initiatives in what we could call basic research, which would include things like learning better ways of developing indicators and measures of success for command and control programs and systems, learning how to better represent command and control in modeling simulations, and things like that. We also have a futures initiative where we look at the future of national security more broadly. Last year we expanded our lessons-learned group. They are actively engaged in looking at Bosnia at the moment, and prior to that, they looked at Haiti and Somalia. We have an in-house consulting group that works closely with joint agencies, organizations, and CINCs and helps them improve their exercises, do long-range planning, address issues related to information warfare, command and control, and the like. We're also involved in developing the implementation plan for Joint Vision 2010.¹ So, we're sort of a full range

¹ Joint Vision 2010 is described as "the conceptual template for how America's armed forces will

from everything from academics to basic and applied research to consulting for DOD clients.

Occasionally we get special assignments from various officials. These three books actually represent special requests. *Dominant Battlespace Knowledge*² stemmed out of a request by Admiral Owens to answer the question, "If we had (what he called at the time) total situation awareness, what difference would it make?" That was the first question. The second book³ reflects a request from Dr. [John] White, who is the current Deputy Secretary of Defense. He wanted something that would explain the challenges relating to defensive information warfare in such a way that it would educate government officials outside the national security community, and engage them in a dialogue to sort out a federal position on this issue. The third⁴ came out of a request by the Chairman [of the Joint Chiefs of Staff], who is very concerned about information being separated from the chain of command and what the impacts on the battlefield might be. Therefore, I undertook a study that resulted in this book on unintended consequences.

We have the luxury of being out of the in-box of the Pentagon and protected by academic freedom, so we can say things that other people can only think, which is useful particularly when you want to think about a future that may be very different than the present.

What I thought I would do today is try to touch upon four subjects that I thought

channel the vitality and innovation of our people and leverage technological opportunities to achieve new levels of effectiveness in joint warfighting." Chairman of the Joint Chiefs of Staff, *Joint Vision 2010*. Washington, DC: Joint Chiefs of Staff, 1996.

² Stuart E. Johnson and Martin C. Libicki, eds., *Dominant Battlespace Knowledge*. Washington, DC: National Defense University Press, 1995.

³ David S. Alberts, *Defensive Information Warfare*. Washington, DC: National Defense University Press, 1996.

⁴ David S. Alberts, *The Unintended Consequences of Information Age Technologies*. Washington, DC: National Defense University Press, 1996.

represented significant national security challenges (figure 1). Tony told me this is a really bright group and that I could basically draw about eight hours down into 45 minutes and you could easily absorb it.

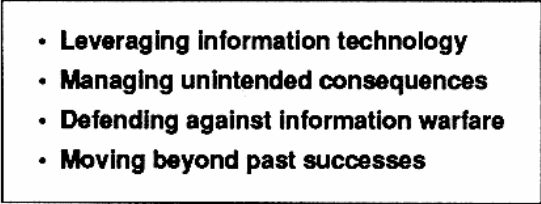
- 
- **Leveraging information technology**
 - **Managing unintended consequences**
 - **Defending against information warfare**
 - **Moving beyond past successes**

Figure 1
National Security Challenges

The first one deals with leveraging information technology, which is essentially at the heart of the debate embodied by the Quadrennial Defense Review. The battle centers around the balance of investments in technology versus readiness versus force structure. You all know the knapsack problem from mathematics: there's only so much you can fit in and something is going to be left behind; the question is, "What?" Managing unintended consequences (the second subject) is about the problem of people, attitudes, time, and tools changing, how an organization has to cope with that, and what the implications are for DOD. The next (third subject) is about the challenges associated with information warfare (IW). I use IW as a metaphor for a whole set of new national security challenges. The fourth and last subject for today is sort of a reflection upon the nature of DOD and what we have to do in order to get a handle on the problems posed by the first three.

Remember, you can interrupt at any time. My teaching career began in the 1960s, and I'm used to interruptions.

Oettinger: With or without Molotov cocktails.

Alberts: At any rate, advances in technology really can have an impact on both the capabilities of the force and on command and control (figure 2). They also introduce

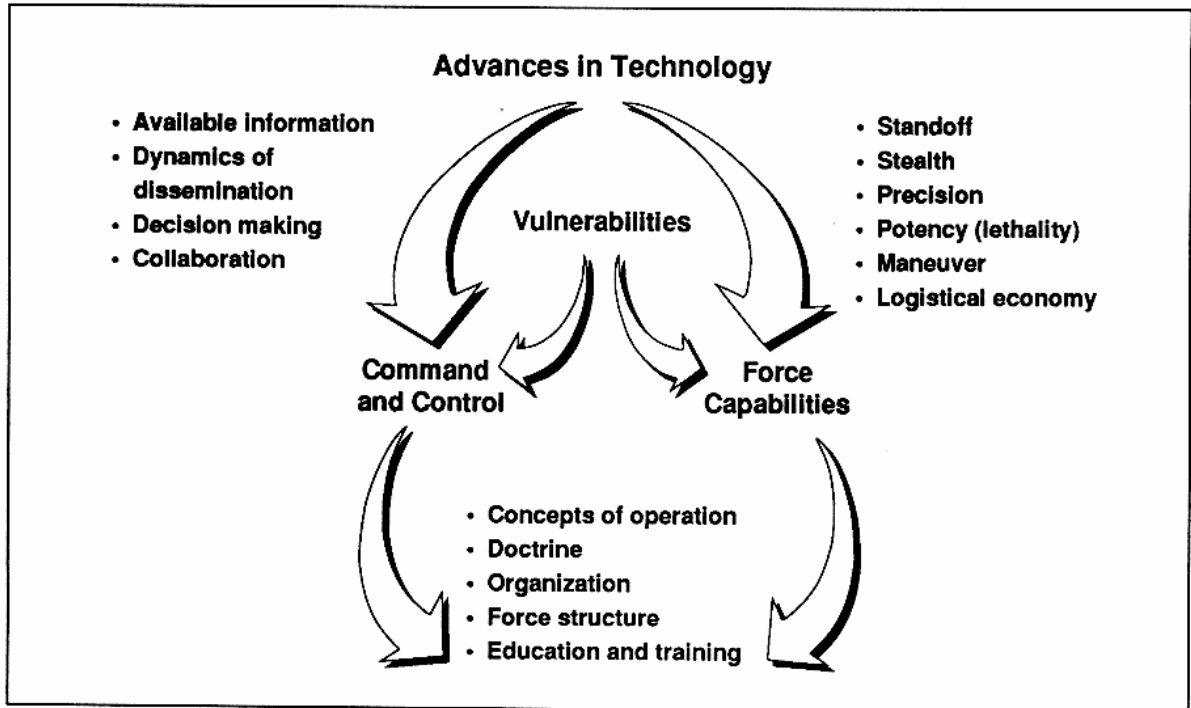


Figure 2
Technology and Traditional War

a new set of vulnerabilities that we have to deal with. If you look at the kinds of things that technology can do in terms of force capability, it, for example, can give us stealth, standoff, and precision. It makes us a lot more lethal when we want to be. In terms of its impact on information, it changes the nature of the information that's available, and it changes the whole dynamics of the dissemination process: who's going to get information, when they're going to get it, and what forms they're going to get it in. So, it has a significant impact on decision making.

Given the coalition nature of many of our operations, the effect that technology has on the ways people collaborate to get their job done really affects how we might approach coalition command and control. My basic premise is that if you change your approach to command and control, then you're going to desire a different set of force capabilities. If you change either of these, then you'd better take a look at your concepts of operation, your doctrine, your organization, your force structure, how you

educate and train, the kinds of people you want to recruit, et cetera, if you're going to make it work.

Now, 90+ percent of our attention in DOD is devoted to what I choose to call "the perfection of traditional warfare" (figure 3). I have come to the conclusion that our ability to perfect traditional warfare is really a function of our ability to understand our environment. If you remember, we have been concerned with the fog and friction of war since the beginning of time. I have always felt that fog and friction were an integral part of warfare, and still are, but there comes a point where you can reduce them sufficiently so that you're in a different kind of decision-making environment, and the nature of your options changes. You get into what I call the simple decisions, where you're basically selecting among a set of known options as opposed to having to generate options to deal with your lack of understanding or your tremendous degree of uncertainty about the problem. Instead of wasting a hell of a lot of time and resources on preparing for a

- **Our ability to perfect traditional warfare depends upon the degree to which we can reduce the fog of war to achieve better situation awareness.**
- **Fog, uncertainty, and chaos**
 - Will always be present on the battlefield
 - Differ by type and significance
 - Are relative
 - Are manageable
- **Expected improvements in C⁴ISR offer us an opportunity to**
 - Significantly reduce the fog of war
 - Reduce the friction in war (more effective management)

Figure 3
Perfection of Traditional Warfare

whole bunch of contingencies, none of which may happen, you can now focus your attention on the things that are most likely to happen. That's a direct result of your being able to "see the battlespace."

Oettinger: How much do you really believe that? Because I have some doubts about what you just said.

Alberts: This is the basic premise that underlies Admiral Owens talking about the 200-nautical-mile cube and the RMA.

Oettinger: So this is not you.

Alberts: This is what I call the perfection of traditional warfare, or the logical extension of increasing our reliance on technology, particularly information technology. The argument is that you've got a 200-nautical-mile cube. You can see everything of importance on the battlefield, and it becomes a question of getting the sensor-to-shooter link. So, we have that opportunity.

Friction is really about telling people what they ought to be doing and getting them to do it. Clearly, if you have better communications with people, and you have

intelligent agents in the form of software that can translate a commander's intent into something people can understand with respect to their assignments and their jobs (which is certainly doable these days), then you can reduce the possibility of misunderstandings and hence reduce friction. Also, if you're not moving people around as much, you reduce friction that's inherent in movement.

We have moved from the notion of "total situation awareness" to "dominant battlespace knowledge" (DBK) because just knowing about something has no particular value (figure 4). If you see a chessboard, you know where all the pieces are, and you know the capabilities of all the pieces, but if you're a lousy chess player, it doesn't make any difference. You can probably be beaten by someone who has a far less clear view of that chessboard, but understands the game a lot better. So the value of improved situational awareness derives from being able to translate that into what I call "option dominance."

How do you do that? If you understand the situation, and can act (as we say) "inside the enemy's decision loop," you're able to see the punch coming before it actually starts, and even if it's on its way, you

- **Improved situation awareness has no intrinsic value in and of itself.**
- **Value derives from parlaying this improved awareness into dominant battlespace knowledge.**
 - Starts with improved situation awareness
 - Continues with improved understanding of the battlefield
 - Concludes with achieving *option dominance*
- **Resources constrained environment demands**
 - Allocation
 - Scheduling
 - Orchestration

Figure 4
Dominant Battlespace Knowledge (DBK)

can be agile enough to counter that in some fashion. As long as you maintain the ability to operate with that kind of agility, you can always choose the time when you want to fight, the place where you want to fight, and the circumstances under which you fight. So, you can basically dominate, in a game-theoretic sense, any option that you're faced with.

Clearly, there are resource problems that have to be dealt with. I remind you of the notion we're talking about: that if you had a hologram on this table of the 200-nautical-mile cube, you could see every target in it, and you could destroy any target in that space any time you wanted. So, for example, there would be no need for close air support, because you would be able to see in plenty of time where the enemy was, what the projection of his weapons was, and when any of your forces were in danger, and either avoid that or call in strikes before the people on the ground actually knew they were in danger. So it changes the kinds of functions that you concentrate on, and it gives you the ability to react in real time to the battlespace.

What does knowledge of the battlespace buy you (figure 5)? It's pretty linear

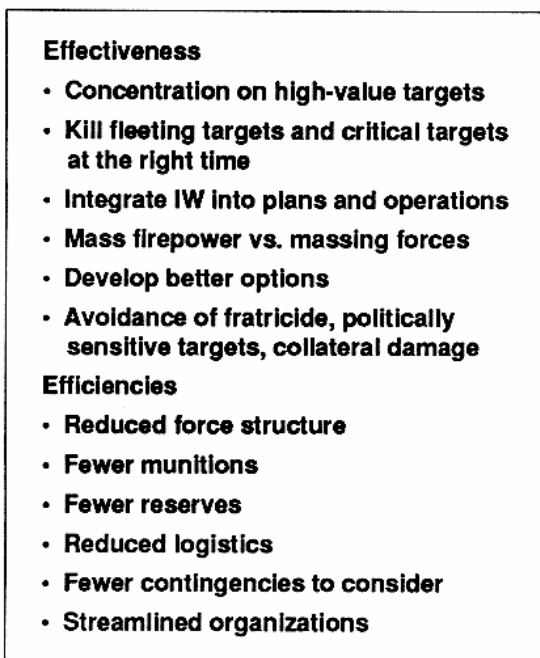


Figure 5
Value of DBK

thinking at this point. Again, you've got a bunch of targets on the battlefield, not all of which have the same value, so what you really want is only to kill the ones that are of high value. That value changes dynamically, so it's not like we're just following command lines or anything like that. There is one particular target that at a given point in time is the most valuable of that set of targets. It could be the difference between hitting a bridge after the enemy has already crossed it, or too soon, so that the enemy can take an alternate bridge, or while they're committed and on the bridge. The name of the game is to hit the high-value targets when they have high value (to us).

We want to kill fleeting targets, things that are moving around, and we need to get better at this. We need to better integrate information warfare into our plans and operations because, since we will have a better understanding of what the adversary's intentions are, we will be able to employ deception and disruption of his communications, et cetera, in ways that are far more effective.

The value of dominant battlespace knowledge also extends to the ability to mass firepower rather than people or materiel, so that stealth and everything come into play there. But stealth and precision guidance don't mean anything unless you know where the targets are.

There has been a trend where intelligence is located in weapons systems. The earlier effective precision guided weapons were laser designated. They required a person aiming this laser in the terminal phase at the target, and thus it kills with great precision. Then, because we didn't want to have to worry about people being there (in close), we moved the intelligence and put it into the weapon itself. The projectile does terrain following, and it can recognize things like decoys and terrain features, and it goes where you tell it to go. That's pretty smart. Both of those things are highly expensive. The second is, however, far more expensive than the first.

We're now moving to a world in which we're taking virtually all the intelligence the other way, out of the weapon. Except for its ability to navigate to a specific spot on the face of the Earth, the weapon will have

little smarts. We're putting all of the intelligence into what we call a C⁴ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) system, which basically spends its time deciding what places on the Earth need to be taken out. So intelligence capabilities are no longer being associated with a particular weapon, but with a system as a whole. I think we learned our lesson after we developed fairly inexpensive weapons, such as Stinger surface-to-air missiles and things like that, and then gave them all to the Afghans to shoot down Russian stuff. Now we worry where the hell they all are. If all the intelligence is in our C⁴ISR system, we know where that is.

Dumb weapons, which anyone can develop out of Radio Shack technology, that can take you to any point on Earth with GPS (Global Positioning System) are now plentiful, low cost, and highly accurate. So we can mass our firepower. Obviously, if we have the luxury of knowing what the enemy is up to, and can see it unfolding, there are certain physics involved that give us an opportunity and the time to develop better options than if we didn't understand all that. Equally obvious, if we know where everything is on the battlefield, we don't have to worry as much about fratricide or collateral damage. It doesn't deal with ID problems when hospitals and command centers are commingled and things like that, but if we move beyond traditional warfare to IW and things like that, we may be able to deal more surgically with those kinds of issues. So, it will obviously increase our effectiveness enormously if we can get this kind of knowledge.

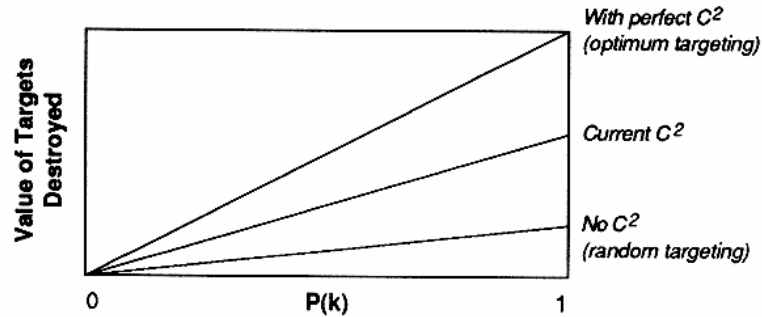
The efficiencies are equally attractive, if not more so, because that's where the budget crunch is. You don't need as many people as you did before because you're not going places. Only the weapons are going places. You don't need as many munitions if they're smarter, and if you're picking out the high-value targets. You don't have to kill 10 targets to get the one you're looking for. You don't need reserves because you know what's happening. You don't need to have this group standing by for some imaginary feint because you see it.

Logistics obviously reduces across the board when you don't need as many people and munitions. There are fewer contingencies to consider; therefore, that saves a lot of time and effort. The organizations are not really streamlined as a function of this, but are forced to be streamlined because the information sort of flows downhill like water, and you can't afford to dam it up at the kinds of places in the organization where it gets dammed up now. Otherwise, it never gets to the shooter, and if the information doesn't get to the shooter, it's no good. So it's now going directly from sensors to shooters in ways that were unimaginable a few years ago.

This chart gives you a simple little example (figure 6). It sort of shows you that weapons still count, and that there's a synergy between the intelligence of weapons and your ability to do command and control. $P(k)$, probability of kill, is nice if it's one. It's not nice if it's zero. Right now, if you assume that you don't have any command and control (and for this example, command and control means you tell people what to do—where to shoot, what to shoot at, what the priorities are, and stuff like that), even though your weapons get better, you're not getting a lot of incremental improvement because you've just got to kill indiscriminately. If your command and control improves (I was generous and put it up considerably from none at all) and if you can sort out to some extent the preferred targets versus the ones you don't care to bother with, then you obviously get greater incremental improvements in the total value of the targets you destroy as your weapons improve. If you've got optimal targeting, if you really understand what's on the battlefield, then every shot counts. Therefore, you get an enormous marginal improvement as your weapons get better.

These tend to reinforce one another, so it's not a trade-off in the traditional sense between command and control and good weapons. The trade-offs come in other areas. So it would not make sense to sacrifice money on intelligent weapons, when the real advantage comes from the *combination* of the intelligence and the precision of the weapons system.

- We can bound the impact of DBK on targets killed as a function of:
 - $P(k)$ s of our weapons
 - Our ability to prioritize targets



- Ultimately, the value of DBK will depend on the degree to which we take advantage of the opportunities provided by changing the way we fight.

Figure 6
Potential of DBK

What does all this mean? It means that a great deal of the grunt work associated with the battlefield gets eliminated (figure 7). The commander doesn't have to worry about feeding the troops. That's taken care of. He doesn't have to worry about his division going off in the wrong direction. He doesn't have to worry where his people are. He doesn't have to worry about where the enemy is. All of those worries get reduced significantly, giving him more time for some thought about the strategic implications of the conflict, and more creativity can result. You have flattened organization structures, which gives you an opportunity to reduce response time.

Automated decisions become possible now. Machines are really good at making decisions where there is not a hell of a lot of uncertainty. They can deal with uncertainty, but it takes a very intelligent expert system to deal with uncertainty. It takes a very simple computer program to deal with deterministic problems, such as route scheduling, target prioritization, deconfliction of airspace, and all those things in which the facts are known. Those programs work really well, much better than

people, so you're going to see a lot of decisions in the future that are made automatically without people thinking about them.

- Strategic/macro assumes greater importance
- Commanders freed to be creative
- Flattened organizational structures
- Automated decisions largely replace staff work
- Increased span of control made possible by automated information flows
- Increased dependence on "intelligent" software
- Emphasis on communications connectivity vs. bandwidth
- Global vs. local optimization
- Commanders need greater understanding of technology

Figure 7
Impact of DBK

If anyone here has ever generated an air tasking order, you know that is a nightmare, and it takes a long time to do it. In the future, it's going to take a lot less time. In fact, we hope it will be done on a continuous basis without the intervention of people, so that you can fly where you want to fly and not worry about bumping into somebody else, or being shot down by your own troops. So that tends to help by increasing tempo and flexibility.

Obviously, given these sets of circumstances, you can control a much broader segment of the battlefield as an individual. However, this also makes you dependent on all this stuff. Therefore, you've got to make sure it works. You've got to understand what its foibles are, and what you do if it doesn't work or if you're subject to information attacks. It places the emphasis on getting a message to everybody. Intelligent processing capabilities will be distributed everywhere. If you go out now to see the Marines play Hunter Warrior in California, they're carrying around little Newtons, and through a little antenna in their helmet, their position and things they're thinking about get transmitted automatically back to headquarters. The bandwidth doesn't have to be enormous if you understand how to compress that, but the connectivity is important because you want to make sure that everybody gets the word.

The last point is that obviously we need commanders who understand technology; otherwise, they're not going to trust it, they're not going to use it, and in fact, they may misuse it. So those are some of the implications of just trying to perfect traditional warfare along linear lines.

A lot of people are scared by that. They would actually prefer to slow down the rate of change in these technologies. They don't understand computers that well. They are very uncomfortable with the fact that the people whom they command have more information than they do, that they may know things that they don't know, that they're not sure exactly what they're thinking. It's a whole different world. Traditionally, all information came from above, and it was shaped and filtered and passed on to shape the cognitive space of the soldiers. Of course, you had doctrine, which is like

preloaded information in people's minds. The idea was that you didn't want them doing anything unexpected. You wanted them to behave in ways that you would hope that they behave. So, this is kind of a scary world.

I basically keep sending the message across that you can't stop the world and get off (figure 8). It's just not going to happen.

- **We can not stop, slow down, control the information explosion or prevent unintended consequences; therefore our challenge is twofold:**
 - Anticipate negative repercussions and take steps to avoid them and/or minimize their impact
 - Recognize and capitalize on unexpected opportunities

Figure 8
The World Won't Stop

Whether you like it or not, this technology is out there. People are thinking in ways that they didn't think before. People will find ways to get the job done outside the formal structure if they have to. If you look at Desert Storm, one of the great pictures from Desert Storm is a soldier with one knee on the desert ground with a laptop, his gun sort of on the side and the laptop right there, and he's playing with his laptop. Now, that laptop is not a normal issue laptop. Those guys brought it because they found that it was useful and they were used to using them. In Bosnia, people showed up with everything imaginable. Of course, there were viruses running rampant through all that stuff—all, to our knowledge, perfectly innocent in the sense that there was no concerted Serb attack on our PCs.

But the point is that people are bringing the tools to their job that they're used to dealing with, whether they're standard issue or not. One is not going to be able to stop that. So, what you have to do is start anticipating what the possible consequences of that are, and try to take steps either to avoid those or to mitigate the damage when it occurs. That's a different way of dealing with the situation than is traditional.

I'll now focus on potential unintended consequences. Here are some of the concerns that are valid to worry about (figure 9). The first concern is that, given the amount of information that's available, isn't it possible that the garbage will drive out the good information? If you get on the Internet, and you ask a question about anything, you're going to get an enormous lot of junk. You've got to sort out the good stuff from the not-good stuff, not only in quality, but also in what's useful to you in whatever job you're trying to do. Clearly, we're not used to dealing with the amount of information that's currently available. We haven't had a lot of practice in it. But this is something that's got to be a requirements issue in the military. People can't sort of go off and say, "Gee, I'm going to

plug into my database back home and whatever I think of I can get a handle on. And, oh by the way, they'll send me updates of all my little profile items." That's not going to work. People have to start spending a lot more time thinking about what they really want, what they would do with it, and experiment with it to get a better understanding of how to leverage that information.

Oettinger: Could I stop you there? Stop me if I'm anticipating something that you were going to do in the natural course of your talk. But it seems to me there's a countervailing phenomenon that gets you hanged afterwards if you follow literally the advice you're giving here. That is: How come you overlooked it? It's the sort of Pearl Harbor syndrome. You get court-martialed the way Admiral Short and Admiral Kimmel did, because in hindsight it becomes clear that there was a good bit of information out there, and you, in pursuing this perfectly sensible recommendation you're making, neglected it. Therefore you're derelict in your duty, et cetera.

Alberts: There are two choices here. There's an alpha error and a beta error. If you don't take this approach, you're guaranteed to fail because you're never going to find the needle in the haystack. Your likelihood of extracting what you really need goes down dramatically. If you take this approach, you increase the possibility that you're going to overlook something or dismiss it before you even consider it, and that subjects you to second-guessing and those kinds of things.

It's got to be a cultural thing. There have got to be norms of behavior that are expected, and that are all part of the doctrine. If the doctrine says, "Filter this way," and you do it, you don't have to worry about retribution. If the doctrine is silent, then you're in a constant dilemma, and if you keep waiting to try to get all the available information, your window of opportunity to act is going to go by, and again, you're going to doom yourself. So, it's just a question of good training and experience.

- **Nonessential information could swamp critical information.**
 - First and foremost, this is an information requirements issue.
 - Next, a system design issue.
 - Finally, a testing, education and training issue.
 - Individuals need to create their own "information domain."
- **Sophisticated presentations could obscure vital information and/or mask the absence or poor quality of data.**
 - Improved presentation (visualization) techniques needed.
 - Also, see above issues.
- **Uncertain information quality and/or integrity could lead to a loss of confidence.**
 - Re: integrity → defensive IW measures, including embedded IW assessment decision aids
 - Re: quality → fusion, decision aids, and presentation issues
 - Re: loss of confidence → education and training issues

Figure 9
Nature and Availability of Information

Often, decision makers tend to procrastinate too long, and so they have no options left.

Student: Can you tell me the working definition of “information” you’re using?

Alberts: Are you talking in terms of “data,” “information,” “understanding,” or “knowledge”?

Student: Yes. The phrase “nonessential information” struck me being sort of self-contradictory if you define information in certain ways.

Alberts: Yes, I use the term very loosely. If you’re saying that if it’s nonessential then it’s clearly just irrelevant data, background noise, and not good. “Information” implies that it has certain utility. Is that what you’re driving at?

Student: Yes.

Alberts: I just used the word loosely. Basically, it could be nonessential for the task you’re doing right now, but important for the task 10 minutes from now. The point is that when you were in an information-starved environment, you were grasping at straws to get whatever you could. Here you will be in an environment in which you’ll have a lot of information, and your job is different. You’ve got to sort out what those essential ingredients are as quickly as possible and not get distracted. So that’s the issue.

The second bullet basically says that the presentations people are putting together are very sophisticated. They are the result of fusion of information from multiple sources and the result of analytic activities that give you not the raw information, but processed information. That’s a very different thing to start to look at than what people heretofore have been used to looking at, which is basically relatively unprocessed information, and relatively simple presentations of what you have. People are going to have to get used to that. Inside the total package could inadvertently be that gem of a fact that you don’t get because the presentation glosses over it, or averages it with something else.

Oettinger: Yes, or you just plain don’t understand it, which was sort of the situation in the *Stark* and *Vincennes* incidents.

Alberts: Those, among other things, they attributed to bad displays, and they’ve changed the displays.

Student: One of the questions about processing the information, as far as fusion is concerned, is that the later it is, the more layers it goes through before the information is actually fused, and the less likely that you gain that situation awareness you’re looking for. Does a lot of thought go into battlefield fusion, single-platform fusion, or would something like a unit that would actually take in more than a single source of information because they had that situation awareness and could do a short-time later real-time fusing of information be tactically useful?

Alberts: I think people are thinking about that in a number of ways. One is clearly to get national asset information down to the tactical level directly in real time. I was just talking to an Air Force guy the other day who reported to me that he actually got chewed out by a senior officer for getting imagery onto an F-16 cockpit in an experiment. The senior officer said, “What the hell would an airman need that for?” Now that they have the capability to do it, people are experimenting with that. Of course, the issue is that it’s hard to fuse at a tactical level, because that means that you’ve got to bring the sources in from so many different places. Each has its own time constants, and the intelligence and processing power needed locally would be very large.

So, obviously one has to balance that. If the only job of that F-16 is to shoot a target, and the pilots just have to know the nature of the target and where it is, then clearly all that other stuff is not relevant as long as somebody else is watching out for the safety of that aircraft, and making sure there are no threats to it. If the pilots didn’t have to worry about that, then they could concentrate on the task at hand. Then there’s always the argument, “Why have an F-16 with a pilot in it, which costs so much

money, when all you want to do is get that target? There are other ways to do it." All those kinds of debates are going on, and they all relate to human processing of information when it's necessary versus automated processing, and when you fuse and take the time and when you don't.

Oettinger: You just said the magic word: balances. You know my fanaticism about that. He's thrown out more balances to be thought about in just the last five minutes than all the speakers in the rest of the semester combined. I'm grateful to you, sir.

Alberts: We're not used to this.

This is an interesting chart on dynamics of dissemination (figure 10). Studies have shown that the same information provided to people in different orders leads to different conclusions. That's really scary stuff. Especially since in the battlefield everyone is now going to be free to reach back to the United States or other resources and get information that they think is relevant to their job. This means that higher-level command posts aren't going to know what their subordinates know or what they don't know, and in what order they got the information. It puts a real premium on making sure that there's a common perception of the situation. Obviously, that's something one needs to work. I've got more of that in the little books.⁵ In the interest of time, I'll move through and just pick out one or two in each one.

Decision making is an issue-rich environment (figure 11). The great fear on everybody's part is that the other guy's going to do the wrong thing. You think, "Gee, my boss is going to give me hell! He's going to look over my shoulder, he's going to see everything I see, and he's going to be

⁵ David S. Alberts, *Defensive Information Warfare and The Unintended Consequences of Information Age Technologies* (see notes 3 and 4); Martin C. Libicki, *Defending Cyberspace and Other Metaphors*. Washington, DC: National Defense University Press, 1997; Harlan Ullman et al., *Shock and Awe: Achieving Rapid Dominance*. Washington, DC: National Defense University Press, 1996.

- **Asynchronous information arrival could confuse and distract.**
 - Education and training needed to avoid pitfalls.
 - Doctrine needed to ensure consistent treatment of information.
 - Display techniques needed to assist in assimilating new information.
 - Decision aids needed to focus attention on essential information.
- **Information imbalances could hamper commonality of perception.**
 - Distributed collaborative tools needed to promote commonality of perception.
- **Real-time automated review could have a chilling effect on subordinates.**
 - New version of old problem
 - Doctrine and associated education and training needed to reinforce good management practices.
- **Uncontrolled or unanticipated use could degrade systems.**
 - Policy, doctrine, and procedures re: use
 - Network tools needed to apply adaptive controls.
 - Design for robustness—just in case

Figure 10
Dynamics of Dissemination

second-guessing me constantly." Now that's a fear. By the same token, the boss could say, "Gee, this guy knows as much as I do. He's going to be second-guessing me all the time. I will be telling him to do this, and he's going to say, 'Why'd you decide that?'" So, everybody's got to get a better understanding of what their roles are, and what their jobs are, and not do other people's jobs. The military actually is pretty good at that. Other organizations and industry tend not to be, but since the middle management has been squeezed out of most organizations, these problems have sort of gone away.

Oettinger: I don't know whether that was an optimistic or pessimistic statement.

- **Superiors micromanage, subordinates second guess.**
 - Organization, doctrine, and training to ensure good management practices
- **Media spotlight affects performance.**
 - Training needed to acclimate individuals to “fishbowl” environment.
- **Collective wisdom stifles innovation and tactical brilliance.**
 - Command and control approach and training to encourage leadership
- **Lack of traditional coordination impacts decision quality.**
 - Collaborative planning and decision aids to provide feedback and red teaming of decisions
- **Desire for near-perfect information delays decisions.**
 - Doctrine and training to improve decision-making skills
- **Failure to accept expert systems leads to underutilization.**
 - Early user involvement in system development and acquisition and training to provide understanding and confidence in these systems
- **Expert systems are not adequately tested.**
 - Operational assessment needed to assess these systems properly.
- **Automated systems fail to recognize their own limitations.**
 - Research, design, testing and doctrinal safeguards needed to prevent failures.

Figure 11
Decision Making

Alberts: Middle management really is no longer necessary in many organizations. Of course, vulnerabilities are all over the place—everything from somebody being able to disrupt, spoof, destroy, or delay information (figure 12). If you’re dependent on information, then it becomes something that you have to start protecting and developing backup plans for in case it doesn’t

- **Sophisticated equipment will be captured and compromised.**
 - Security features, doctrine needed to prevent exploitation of lost equipment.
- **Increased reliance on COTS increases vulnerabilities.**
 - Defensive IW plan, design and acquisition strategy needed to minimize exposures.
- **Growing sophistication increases threat.**
 - Same as above
- **Difficult to detect penetration and its consequences.**
 - Embedded defensive IW decision aids needed for detection and evaluation of attacks.
- **Cost of a single penetration can be very high.**
 - MEII, damage control techniques needed to contain damage.

MEII = minimum essential information infrastructure

Figure 12
Vulnerabilities

come across. If you’re used to getting along with nothing, then you’re used to operating that way, but since the whole philosophy of how one’s going to approach a battle is going to change, it becomes even more important to make sure that the assumptions, the foundations, upon which this new approach rests are realistic and stable.

It is surprising how few exercises are done in the military that play information warfare against themselves. In effect, what they’re doing is saying that, “We’re going to assume that all this stuff works. Now we’re going to learn how to use it.” That’s clearly a first step. Obviously, you have to learn how to use it when it’s available, but it’s equally important to learn what you’re supposed to do when it’s not available, and that step we haven’t taken yet. This is clearly something that we’re going to need to put a lot of stress on, at least in raising people’s awareness of this.

There's a tendency not to want to screw up an exercise because you get criticized for it. Until there's a general understanding that that's not screwing up the exercise—that is, in fact, what the exercise is all about—people are going to be reluctant to do these kinds of things.

This all has implications for design and acquisition (figure 13). There are lots and lots of things here. We'll go through some of this a little bit more when we talk about information warfare. Clearly, one of the major things about design and acquisition is

- **Traditional T&E approach mismatched to needs**
 - Holistic, integrated, operationally oriented process needed to expedite fielding of capabilities.
- **DOD capabilities to fill COTS gap diminishing**
 - Focused, coherent research programs needed to avoid shortfalls
- **Adversaries will improve their C² disproportionately by exploiting COTS**
 - Need to study competition and incorporate results in MCP concept and system design
- **Inadequate resources allocated for post-deployment "O&M"**
 - Life cycle planning needed to ensure adequate resources.
- **Ability to maintain continued interoperability with evolving COTS components**
 - Need reengineering for acquisition approach → COTS Corps
- **Readiness impaired during transition**
 - Mission-based strategies need to phase in new approaches
- **Commercial capabilities may not be available to the extent required due to global competition (e.g., bandwidth)**
 - Backup, degraded mode contingency plans, training, and realistic exercises needed to ensure continuity of operations

Figure 13
C² Design and Application

that, given the profound change in the nature of the job and how you're going to do it, it doesn't make any sense to assume that you know everything you want your systems to do five years before they get delivered. So obviously, you're going to have to take heed of the advice of those of us who have been advocating evolutionary design and acquisition systems, where you learn and you test as you go along, and you make appropriate adjustments.

Each and every one of those possible problems has a remedy, and if you look at all the remedies and look across them, you come down (not very surprisingly) to these things (figure 14). You obviously have to educate people and organizations and train

- **To address each specific concern, attention must be focused upon one or more of the following:**
 - Education and training
 - Doctrine and concepts of command/operation
 - Technical requirements
 - System design
 - Organization
- **Acquisition reform, particularly T&E, is a prerequisite for success.**
- **Research is needed for selected remedies.**

Figure 14
Nature of Remedies

them to deal with this new thing called information. You have to teach them how to operate in an information-rich environment. You have to teach them how to operate when that environment's degraded. You have to come up with new concepts and new doctrine to deal with it. Obviously, if you've introduced a new information system and now you have a guy who was supposed to make a decision, who no longer has the best information available because someone else has it, then somehow that decision authority has got to change, otherwise you've got some really dysfunctional aspects to your organization. Obvi-

ously, research is needed because I need to have a job, but also because we don't know the answers to these things.

This chart just deals with the fact that no one remedy can totally address any of these problems (figure 15). You're going to have to orchestrate and coordinate remedies. When you change the organization, there's an implication for doctrine and training, et cetera.

- A number of remedies are needed to address each concern.
- Remedies must be coordinated with one another.
- Remedies must be integrated with existing structures and processes.
- Integrating remedies may require changes in existing structures and processes.
- Close collaboration among responsible communities needed.

Figure 15
Orchestrating Remedies

Oettinger: May I stop you, because you made (rather lightly, I thought) an earlier statement about the disappearance of middle management. I see here a recipe for reintroducing sort of new kinds of middle management that will be called orchestrators or remedies integrators and so forth. There are an awful lot of simple-minded notions about the "information revolution," which neglect the magnificent set of considerations that David has put in front of us here. He's giving us a beautiful checklist, and if you guys take nothing else away from this course, save these foils, because they put you 10 light years ahead of most folks in the private sector, as well as in the military, who never come near thinking in such detail and such exquisite precision about the issues that arise in what others tend to lightly wave their hands at.

Alberts: In the next couple of slides, I'm sort of going to talk about how we will in-

roduce change into DOD. The words have evolved a little bit since these slides were made. Clearly, you need an approach that allows you to coordinate a coherent set of remedies to these problems (figure 16).

- We need a process to facilitate the close collaboration required to put together a coherent set of remedies and integrate them into existing structures and processes, making necessary changes to these structures and processes.
- When structures and processes are tailored to accomplish specific mission(s) they can be thought of as mission capability packages.
- A mission capability package coordinates all the elements needed to field an operational capability successfully.

Figure 16
Approach

The real challenge is that those remedies are the province of different people. There is no one in charge. At the very highest level there is, but they're worried about other things. But at the working level, the people who do doctrine are not the people who buy systems. People who buy systems are not the people who educate our military and our civilians. So, you have all these people who are more or less independent stovepipes who have to get together somehow in order to get something done, which, of course, doesn't happen. I was faced with the problem of trying to invent a process that was going to make a lot of people unhappy by impinging on their freedom of action. I think we've actually succeeded in doing it.

Oettinger: I don't believe that you're still alive!

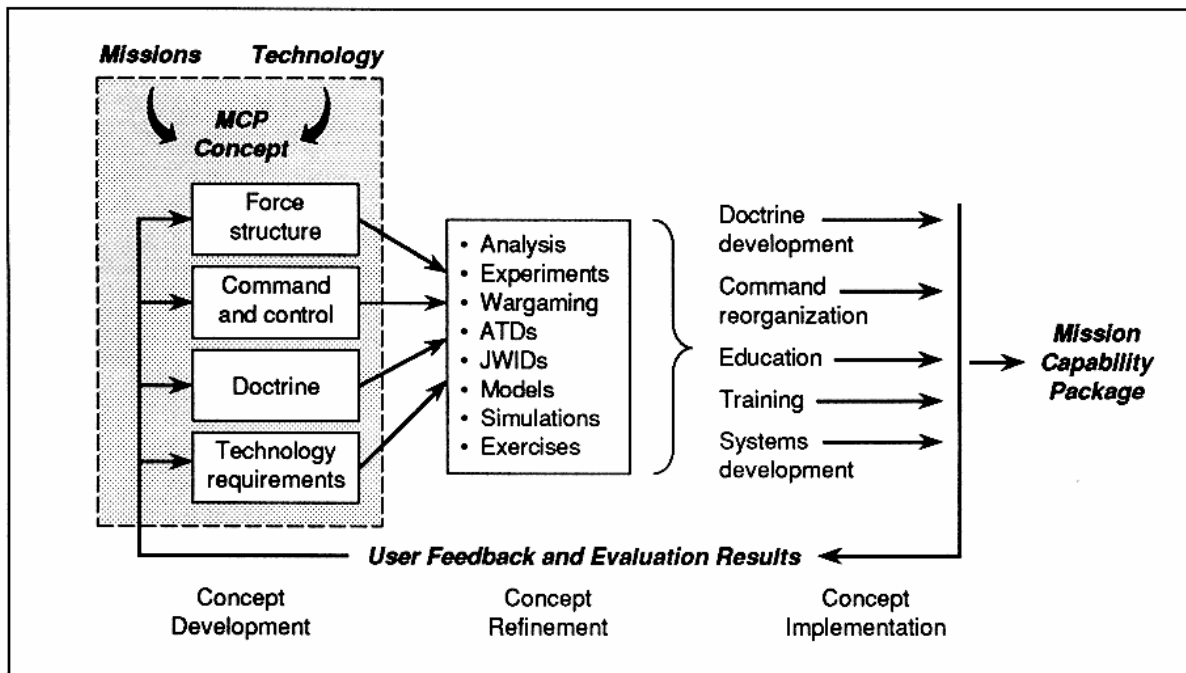
Alberts: They're not aware of it yet. What we decided to do is what we've now called basically the "coevolution" of all these considerations—the simultaneously iterative

changes to doctrine, organization, culture (if you will), systems, information flow, devolution of responsibility, weapons capabilities, and everything all at the same time. We call them mission capability packages (figure 17).

Basically, if you came on the scene a few years ago, the way technology was inserted into military organizations was quite simple. The technologists would come up with these great new ideas, and they would go out and demonstrate them and get people to say, "Yes, that's pretty good stuff." Then they'd ask people in the operational world, "Do you like this stuff?" and they'd say, "Sure. It can help me do my job, so I think it's a great thing." What they meant by that is, "I could do my job exactly as I'm doing it today, but a little bit better. Instead of taking the paperwork and going over to another office, I can now send an e-mail over there. Of course, I still have the 23 steps to process the paperwork, but now

it can be done faster. I like that." That's the way they did it. Never once did that person in an operational job think ahead to say, "Gee, if I only had this, I could change how I approach my job. Let me go talk to the technology people and see if maybe they could actually give me this." Those kinds of conversations never took place.

So the idea was to go back and create a collaborative process by which we would bring people who wrote doctrine, people who thought about organizations, educators, and technologists together and say, "Look, first we're going to give you a briefing by the technology people. They're going to tell you what they'll have available 10 years from now. This is what they can do for you. Now, you can say, 'I don't need that stuff,' or you can say, 'Well, I sort of need that stuff, but I really would like this instead,' and then a conversation starts."



ATDs = Advanced Technology Demonstrations
 JWIDs = Joint Warrior Information Demonstrations
 MCP = Mission capability packages

Figure 17
 Mission Capability Packages

Admiral Cebrowski⁶ and Anita Jones (she was here last week) started a thing called ABIS—Advanced Battlefield Information System. I don't know if she talked about that. But the notion, and this is just a start, is to get the operational community and the technical community together to think about the future. What is the battlefield going to look like? Who are the enemies going to be? What are their capabilities? What can the technologists bring to the table? Then they can develop a concept about how you're going to do that, and start, at least on paper, to do it.

Let's just assume that the technologists deliver what they say they will deliver, and then see if it resonates well with people. If it does, we'll do some analyses and see if this is really feasible—order of magnitude kinds of things: can we afford to do this, is it really going to work, et cetera. We'd start going through a whole bunch of things before you get to the point where you actually have the technology to demonstrate, because when you finally have it there, then we need people who thought about it, who will now use it in a way that's different from the way people do it today. So we would go through this process.

Now, what does that give you? It gives you an opportunity to see what the unintended consequences are, because you're now playing with it in advance (figure 18). You can say, "Gee, if we do this, Joe over here has got to make this decision. He doesn't have the right information. It's all on paper, it's all in test beds, it's all in models. Now all I have to do is sit down, hit a couple of keystrokes, and the person's got the right information, and we try it again." So you learn all of that before it's cast in concrete.

It's sort of like the Boeing 777 design. Tony said he was going to get all the tapes for future classes. If you haven't seen that

⁶ VADM Arthur K. Cebrowski, Director, Command, Control, Communications, and Computer Systems (J-6), Joint Staff, 1994–1996. See his presentation, "Command and Information Systems," in *Seminar on Intelligence, Command and Control, Guest Presentations, Spring 1996*. Cambridge, MA: Program on Information Resources Policy, Harvard University, January 1997.

- **Unintended consequences can be successfully managed by introduction of change via mission capability packages.**
- **Remedies cluster around education, training and doctrine and require acquisition reform and research.**
- **Start thinking and talking about the future in terms of mission capability packages.**

Figure 18
Summary

series of tapes on their design development process, you should, because it shows how they revolutionized design in building airplanes. They undergo a similar process. Instead of the mechanic finally walking in and wanting to put in the rudder assembly and finding that it's blocked by the fuel line, that's all done by computer a long time ago. Three-dimensional graphics, CAD/CAM (computer-aided design/computer-aided manufacturing) programs, all sorts of intelligent software looks at how this plane's going to be built before it's actually built, and identifies conflicts and things like that.

Oettinger: That raises some other interesting and unresolved questions. I mentioned over lunch a former student, Matt Bencke, who is now with Boeing, who also did a book on U.S.-Soviet space and the cooperation and competition.⁷ He gave a talk a couple of months ago at the Russian Research Center here, and it precipitated a discussion with the assembled Sovietologists. *À propos* of it is this: Russian design doctrine in the aerospace business is very different from ours. That is, we have a long tradition of doing paper designs, of which this 777 thing is just a culmination. What they would do is make six of the damn things, and if three of them crashed, big

⁷ Matthew J. von Bencke, *The Politics of Space: A History of U.S.-Soviet/Russian Competition and Cooperation in Space*. Boulder, CO: Westview Press, 1997.

deal! You've got three others still working, and you're ahead of the game because now you have a proven design. You've got working models. From the discussion around the table it was not clear, given the high cost of software and the high cost of modeling, et cetera, that the paper design technique was necessarily and also economically or operationally better than making six or seven of the darn things, and ...

Alberts: ... skipping the design phase.

Oettinger: Well, yes, or a much lighter design phase and much more emphasis on making the actual things and making your mistakes on the real thing and crashing a few of them.

Student: Don't you think that's partially cultural, though? If Boeing made six 777s and three of them crashed, no one would buy them. But if Tupolev made them, Aeroflot was going to have them because it was required.

Oettinger: You're absolutely right. I'm simply pointing out that you have to step back and say that this is not necessarily the only way to do things. This is only one example, under one set of cultural circumstances, when an alternative proved quite competitive in many ways. Among other things here, we're now buying Russian ejection seats. They've got the best darn ejection seats in the world, and they were not produced by Boeing Corporation. I don't know how many people fell head-first. One has to be careful. People on bicycles do run rings around us, occasionally.

Alberts: I think that we're going to find that the software tools will decrease in cost. Building a 777 just to see if it works is going to be far more expensive than that. But we're doing this playing with something not as simple as the 777. These are complex adaptive systems, because there are lots of people with different perspectives and different agendas, et cetera.

The other point is that all of these guys have sort of been in the process. In the old days, they'd test it and then they'd say,

"Let's field it," and then the doctrine people would be starting from ground zero. Nobody ever heard of this thing. Nobody knew what to do with it. Here, the doctrine guys have been in since its inception. So in order to get doctrine out on the street, it's a lot easier than if they finally came in and just saw that. They're not exactly your most forward-thinking elements of your organization, necessarily, although sometimes they are. Sometimes you can get lucky and the doctrine people are way ahead of the rest of the force. The point is that they should be with the whole process. You end up with an implementation phase that goes much faster, and you get something that we call a coherent package where everything sort of meshes and works well together, and you have less likelihood that some unintended consequences can come up and bite you.

The other thing that I didn't mention, which is equally important, is that there are going to be opportunities to do things in ways one never thought of, and it's a good idea to identify those in your early stages rather than in the late stages. They will have implications across the board. This chart (figure 18) basically just says that you can manage it, and you should manage it using this sort of integrating approach. It's not managed from above, which isn't going to work really well, but it's a collective effort.

Student: Sir, a question about that exact point. If those mission capability packages are the unifying vision that gets all these disparate communities together, who decides what mission capabilities are necessary?

Alberts: Regarding Joint Vision 2010, we have a Joint Vision 2010 working group, and their job is to do the implementation plan. Earlier this week, I presented them with the vision for their long-range planning approach. Basically, it's very similar to this chart (figure 17). The notion is that they're going to take different missions and assign them to different people who will have responsibility for carrying out that mission. That designated person will then, obviously, have to pull together a team that

has the doctrine component, the technology component, and all of that, and be responsible for putting them together.

The way we force that, if you want to use the word “force,” is that we’re creating milestones on the implementation plan that show that they have achieved a certain operational capability, not that they’ve demonstrated some technology or other. We’re sort of forcing the milestones to be something that either has to be a proof of concept, or a demonstration, or an achievement of a capability. We’re going to the end and saying, “We’re going to measure you based upon your putting together this package. We’re not going to measure you on pieces of the package.” In effect, you’re delegating, but you’re also giving them guidelines for how they’re going to pull that together. So, it’s sort of managed, but it’s not. That’s the way the Joint Staff works.

Student: But somebody in the Joint Staff is saying, “These are the seven mission capabilities we want.”

Alberts: Oh, yes, the Chairman’s going to say that. The Joint Staff is going to assign it, but they’re not going to tell them how to do it. For example, there are four of what they call “enhanced operational concepts”: focused logistics, full spectrum dominance, precision engagement, and full-dimensional protection. That’s one dimension of a cube (figure 19). Another dimension of this cube is all the things I just talked about: the mission capability package. So you have a cube in which you have the elements in the mission capability package; you have those four things that are in Joint Vision 2010; you have the mission spectrum which goes from nuclear war through MRCs (major regional conflicts) to operations in peace. Then there’s information superiority, which is the foundation of all.

To make a long story short, you can slice up this cube in lots of different ways, and whichever way you slice it up has implications for what you have to connect to later on. But if you take a slice out of this cube, then you’ve got another shape, and

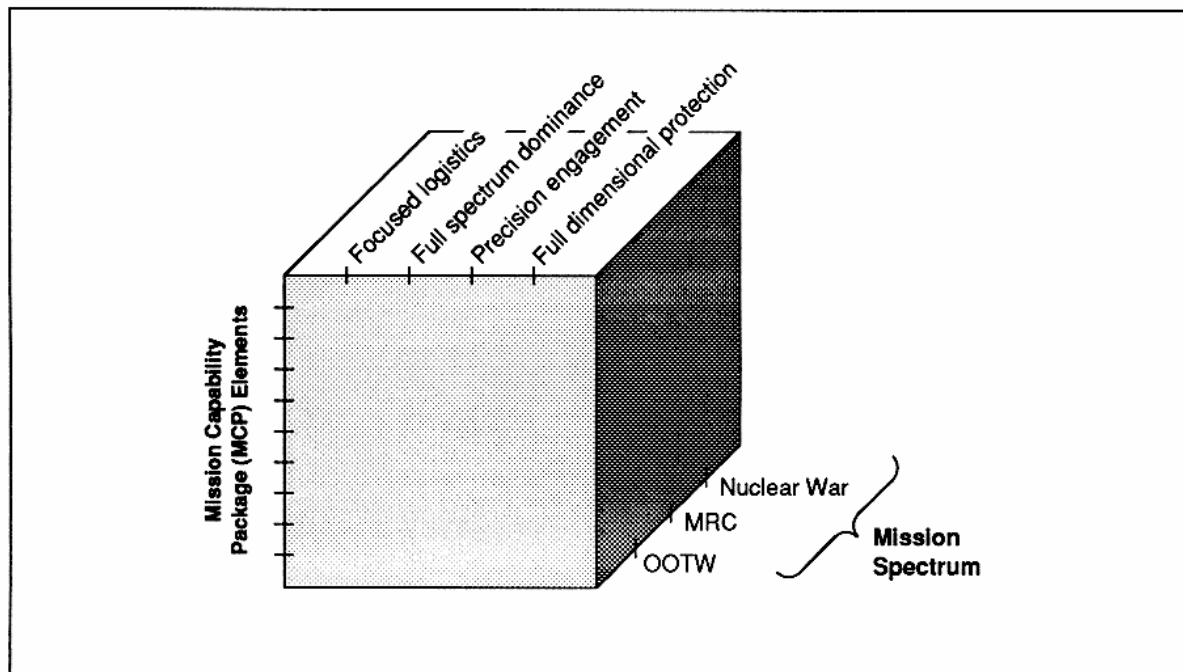


Figure 19
Creating an MCP

that shape has a PERT (program evaluation and review technique) chart associated with it. If you do that for all those different elements you will have this hierarchy of PERTs, and through that there is going to be the Chairman's integrated path with critical milestones that will, hopefully, be strategically selected so that they measure the results of mission capability packages rather than the components. Every year there might be 12 of these events, and what that means is that the communities responsible for the pieces know they have to work well and play well together in order to get there. Everything—Congress, the Chairman, and everyone else—is going to be focused on that. It's not that there is a direct line of authority and all these guys are being smooshed together, but their objective function is being managed. That's got a chance of success.

There are still a lot of arguments at the meetings. People don't argue about this stuff; this makes logical sense to them. What they argue about is the relationship between overseas presence and dominant maneuver and stuff like that. All that is very abstract. If they start to have to focus on specific things, like "Here is your scenario, these are how many targets you're going to have to engage, this is how you're going to have to get the forces deployed, this is how you're going to have to do it," obviously, that implies that they need an organization designed to accomplish that as efficiently as possible. They have to develop the doctrine to go along with it. They need to train the people. They need to get the systems in place, or at least, in the early stages, postulate what those capabilities are. So they're being forced to integrate intellectually across that space in order to play in the game.

Hopefully, it will work. It's just too big an organization, with too many institutional sets of culture and inertia to sort of use the heavy hand of dictatorship to get it done. It just doesn't work.

Oettinger: By the way, I think that what Dr. Alberts is saying is an interesting indication of progress. If you go back a couple of years to Admiral Owens' presentation

here at this seminar,⁸ I think you'll find statements to the effect that one of the aims in overstating somewhat (to my taste) the Revolution in Military Affairs, et cetera, was to stimulate this kind of thinking. In that respect, you're starting off with a very traditional, hidebound view. The notion that such discussions are now taking place, presumably with more or less real people out of the services and so on, is a significant mark of progress.

Alberts: Look, it took 18 months to get Joint Vision 2010 out of the building, and that's just a piece of paper. It would be nice to focus people's attention on doing real things.

Student: It sounded as if the four processes you identified that are going to allow us to set up 2010 are all things that are already being done, but being made more efficient—maneuver, logistics. Are those where those people are coming from to make these agreements?

Alberts: I told you that 90 percent of the efforts focus on perfecting traditional warfare in that sense. I don't agree with that, but that's the fact. But if they can do it this way, then they may find out that they can do it with a lot less resources than they think.

Student: The people who are in these groups are coming out of those functional organizations in the services?

Alberts: Oh, yes, absolutely. For instance, the J-4 is getting responsibility for focused logistics.

Student: So, if you were to make a group like this for information warfare, strategic attacks that you can make with your information systems, whom would you pull?

⁸ William A. Owens, "The Three Revolutions in Military Affairs," in *Seminar on Intelligence, Command and Control, Guest Presentations, Spring 1995*. Cambridge, MA: Program on Information Resources Policy, Harvard University, January 1996.

Alberts: That's a very good question. At the moment, the J-6 would do the defensive side, the J-3 would do the offensive side, and the J-2 would support both of them, I guess. But they're not thinking that way yet. We haven't gotten to that point.

They just took command and control out of this chart (figure 19). My earlier charts had it. But command and control and information superiority were two things that went around, and that's because I wanted to stress the importance of command arrangements, one of my favorite subjects. I guess that people felt that that gave J-6 too much power, so they sort of got rid of the command and control, and they just call it information superiority now, which is a ubiquitous term that everyone can live with. But the notion that you would take something as vital as command away from the J-3, and turn it over to some wireheads, is something that makes their blood run cold. That sick notion about J-6's comm guys is also out there and has to be dealt with.

This is a good lead into the next section of the talk, which is about information warfare. It's also a good lead in because what I worry about is not information warfare *per se*, but nontraditional threats.

My concern is that there are other threats to national security that are far more likely and just as devastating as the more traditional one. Digital warfare is one of those things (figure 20). It's not the only one, but it's one that I think has a lot of characteristics that it shares with 21st century kinds of threats.

My feeling is that if we put all our eggs in one basket—tanks, ships, planes, and things that blow up—we're going to have the equivalent of the Maginot Line, which can be flanked with the speed of light, and we're not even going to know it. Digital war has all the wonderful characteristics of what we're seeking to achieve in traditional warfare. You can't think of any attack that would provide us with less warning than an information attack. We might get some strategic warning, but we're not equipped to deal with that in the intelligence community really well, although we're trying to catch up. You certainly can't see electrons

- **The 21st century may see a new form of strategic warfare.**
 - Many of the same objectives as before, but a different way of going about it
 - Reliance on traditional concepts of operations and weapons may be 21st century Maginot Line
- **Characteristics of "digital war"**
 - Little warning, low-cost info bullets (PGMs), ultimate in standoff and stealth, no "forced" entry
 - Loss of sanctuary
 - Traditional military response unacceptable/ineffective
 - Perception of vulnerability may exceed actual damage

Figure 20
"Digital War"

massing at the borders. If you did, you wouldn't know whose electrons they were, anyway.

The bullets are really low cost. Think about a computer program. Once you develop it, it reproduces itself *ad nauseam* for virtually no cost. Can you imagine somebody inventing a way to produce one tank and sort of have it grow, like in "Fantasia"? That would be just an incredible thing. So an information attack doesn't cost much. Standoff is great. You can be anywhere. I was at a meeting a couple of weeks ago where NSA was showing us new ways to attack systems, and it's pretty much fun, right? (Actually, they were showing us old ways. They didn't show us the new ways. They were just demonstrating that there are well-established ways to do it.) But you can do it literally from anywhere, and the traces are almost nonexistent. People are working on that now, but it's not like you see the lock's been forced. You can't see a digital attack if it's done well. So, we've got some real problems.

Student: Doesn't that somehow tweak the perception of dominant battlefield knowl-

edge? That reduces it to sort of visual domination.

Alberts: Yes, that's always a problem. Admiral Owens always kept talking about the 200-nautical-mile cube and targets. You could only infer intentions, and all of this stuff that's less readily seen was not envisioned. Clearly, you can see somebody's command network, not only physically but also from its emanations and things like that. You can do traffic analyses. There are all sorts of things you can do. It just makes it harder and harder and harder. What's one message versus another message unless you're actually able to read the message? That's why we're really up tight about the whole encryption stuff. We don't want messages going around we can't read. It's inevitable, but we're really trying to be what's-his-name with his finger in the dike on this. It's just not going to stop it. But that's why we're concerned.

Oettinger: It's the little Dutch boy. Did he have a name?

Student: I don't think so.

Alberts: There is a great deal of skepticism about how real information warfare is, what people can actually do to each other, and whether or not anyone really intends to do this to us (figure 21).

This is really funny. After I was a professor, I took a job with the Lindsay administration⁹ and ended up in the police department. So I saw both sides of the 1960s. In any event, my feeling was that that's where I learned means, motives, and opportunity and all of that because I got to reorganize the detective branch. Those exist, and there's no question about it. The means are there. The motives are everywhere. Our vulnerabilities are so bad that the opportunities for real havoc exist, and it's getting worse.

Now, when I face someone who really pushes me to the wall and says, "Well, have the North Koreans done anything to

⁹ John Lindsay, mayor of New York from 1966 to 1973.

- **IW attacks are a fact of life: significance being debated.**
- **Technically feasible "strategic" threat exists.**
 - Means, motives and opportunities exist.
 - Well-planned, coordinated attack could
 - thwart foreign policy, degrade military performance
 - damage economy, undermine faith in government
- **Cannot wait for "validated" strategic threat (e.g., smoking keyboard) to take prudent actions.**
 - Reactive solutions only encourage more attacks and are expensive.
 - Proactive approach is needed.

Figure 21
Current Situation

the South Koreans yet? Do you know what they're going to do?" of course I say, "No, but I think it would be somewhat imprudent not to sort of assume that they could do things that we would not be happy about." But I'm really thinking not about today, but about 10 or 15 years from now. I'm thinking about the increasing complexity of our infrastructures, particularly our information infrastructure and the command and control capabilities that are built on it. With this increasing complexity there comes a certain amount of chaotic behavior. I don't know how many of you have studied complexity theory and all that. It's probably worth an hour of your time to get a quick primer on what complexity theory is, and what chaos is all about, because it's kind of relevant to a lot that will be happening over the next couple of decades.

In any event, without someone getting a handle on those, we could be in trouble. We could be our own worst enemies by putting together systems that have inherent instabilities in them that we don't discover until something goes wrong. We'll be committing acts of information warfare on ourselves. So, the very actions we take to prevent systems from spinning out of control, and to let them recover from damage of various kinds, regardless of whether it

occurs inadvertently or not, are the same kinds of things we would do to protect ourselves against an adversary. So, it seems we have more than one reason to start to pay attention to this.

Student: Couldn't there be a flip side to that? As the systems become more and more complex, that bullet about making a well-planned, coordinated attack also becomes much more difficult in terms of defining the intelligence to achieve the objective of degrading military performance or damaging the economy.

Alberts: There is a difference between complexity and interdependence. What's happening is that they are getting complex in the sense that we don't understand it. That's true. The argument goes that we're doing this so that our adversaries can't understand it either, and there is all this redundancy and that brings along a certain amount of robustness.

The truth of the matter is, the complexity is coming from the interdependencies among all these systems and between systems of one infrastructure versus another. The infrastructures that run telecommunications and power have interrelationships. We could be pretty good in telecommunications, but if the power grid goes down, we're in trouble. We didn't figure out that there are relationships between those two, and that's because there are things called SCADA (supervisory control and data acquisition) systems, which underlie all of these infrastructures. They are information systems unto themselves, and they talk to each other and everything gets related. For example, the power systems are dependent on the telecommunications system to keep in balance and all that kind of other stuff. If one got hit, the other could go down. If you don't have the power, you're not going to have the information systems to try to reconstitute them.

Now, we really don't understand this, but (and I'm not saying this as a joke) we have a presidential commission that is looking at the interrelationships among infrastructures and their vulnerabilities. It's called the President's Commission on Critical Infrastructure Protection.

Oettinger: Established by Executive Order 13010.

Alberts: I understand your arguments both ways, but I think that I would come down on the side that complexity will lead to occasional catastrophic failures unless the design is properly done to isolate different parts of that system from the effects that occur in other parts. You're all too young for this, but when I was in graduate school, the whole power grid on the East Coast went down. Nobody expected that. It was a cascading effect of events.

Oettinger: There's a good account of it in a paper by Sid A'Hearn.¹⁰

Student: Basically, you're saying that complexity is going to make defense more difficult than it is targeting for offense. You would be able to find these cascading nodes offensively fairly easily, but understanding what the effect of the cascade is defensively may be fairly difficult to do.

Alberts: I don't think I'm saying it makes either offense or defense more difficult. It makes us more vulnerable to inadvertent events causing problems. Now, it may or may not make it more difficult for the offense. If you think about it, it actually makes it easier for the offense. All they have to understand is first-order kinds of things, and they could hit a series of things that get some synergy going and cause us all sorts of problems. If you thought it out, you could do a lot of damage.

Student: But you wouldn't have much understanding of exactly how much damage you're going to do.

Alberts: That's right, and that's another issue that we'll get to. Not only won't the enemy know how badly they're going to

¹⁰ Francis W. A'Hearn, "The Northeast Power Failure and Lyndon B. Johnson: An Interview with Donald F. Hornig, June 30, 1983," Incidental Paper I-83-3. Cambridge, MA: Program on Information Resources Policy, Harvard University, October 1983.

hurt us, we're also not really going to know. The real damage is going to be psychological to some extent, and not actual. Whenever I go on a trip, I hear my dear colleague Martin Libicki on CNN or something, and he'll say things like, "Washington shuts down every time we get three inches of snow." We can deal with that. The truth of the matter is that we all understand a snowstorm. We're not going to run to the bank and take our money out. But if these kinds of attacks are not handled well by the government, it will lead people to believe that the government is not able to provide a reasonable set of conditions under which we can prosper, and that's going to create all sorts of tensions.

At any rate, what I'm saying is that I do not want to wait for Pearl Harbor to occur. A digital Pearl Harbor is the thing I hear people wringing their hands about in the Pentagon, "Well, nobody understands this. We're just going to have to wait." That's pretty self-defeating. It's going to happen. It's a question of being prepared.

Student: If we're so woefully unprepared to fend off or even to notice this sort of attack, what's the rationale for increasing our dependence on software systems for our own defense and for offense? If we're talking about dominant battlespace knowledge and giving these incredibly enormous computer programs a great deal of intelligence and really a great deal of responsibility, doesn't that seem sort of counterproductive if these very same computer programs are so vulnerable?

Alberts: That's a good question. First of all, not everyone believes or accepts that they are as vulnerable as I'm implying they could be (or they are, actually). That's one.

The second thing is what I said about progress. That's going to occur. People will continue to depend on these things. Now, there have been incidents where tens of millions of dollars have been lost, stolen, embezzled—hundreds of millions a year, even billions a year, if you add up all the IW-related damage that occurs—but it's absorbed within a larger economic institu-

tion. The only large institution that has admitted the problem is Citibank, and they have an expensive program underway to deal with that. The others, I think, are working on it, but there's a problem. They don't want to admit they have a problem, because if they admit it customers may not trust them anymore.

In national security you have the same kind of problem. We don't know how bad it would be because we've never suffered such an attack. We don't really have a good handle because we never even exercised attacks like this. But it's clear that the military doesn't have its own infrastructure isolated from the society as a whole, and so, it depends on other systems. Ninety-five percent of all communications goes through commercial switches and satellites and all that kind of stuff. The emergency response stuff, the logistics to get us from wherever our stuff is to ports and onto ships and out of here, is mostly commercial infrastructure. For that reason, it could undermine our ability to deploy troops.

Oettinger: Ninety-five percent is not accidental. In the Soviet Union, the military networks were very carefully segregated from the civilian, and the political consequences of that are a whole other matter. So the intricacies of the choices that need to be made here and the balances to be struck have major ramifications in a number of directions.

Alberts: We sort of did information warfare to Iraq to a large extent in the more traditional notion of counter-command and control and stuff like that—C²W.

The really scary part is that you can have attacks directly on citizens' ability to function in society without going through the military, and without the military being able to interpose itself between those bad guys and our citizens (figure 22). This is true whether you take IW out and you talk about terrorism, or economic warfare, or cultural warfare, or all sorts of potentially new forms of influencing society or taking away their appetite for intervening in

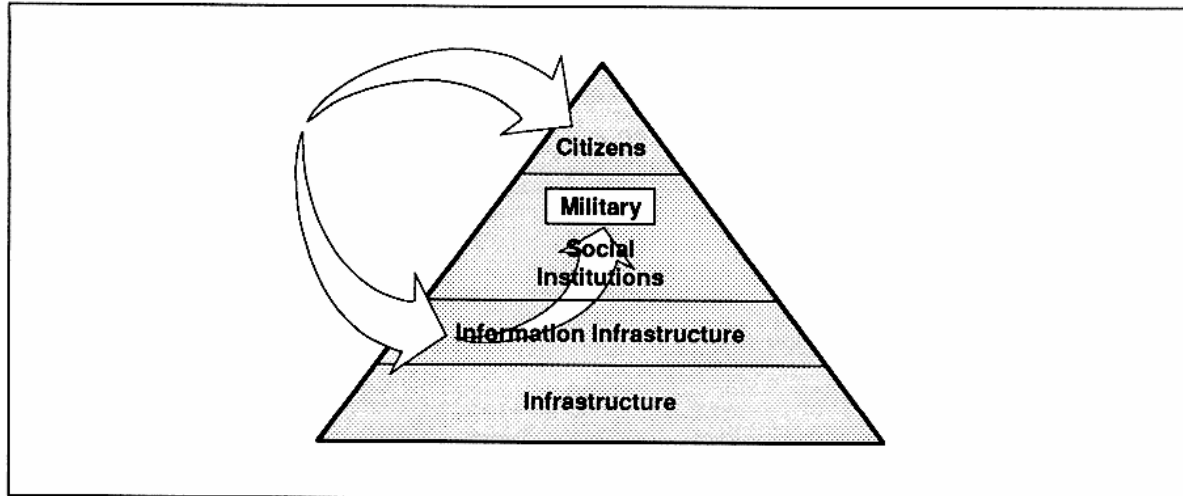


Figure 22
Strategic IW Attacks

another part of the world or all sorts of things. You have a situation where people can attack in ways that were just not possible in the past.

Student: An episode that I lived through last year was that an e-mail was sent that eventually made its way to Scott Air Force Base. It was an e-mail chain letter: "This little girl will be saved because we're going to collect so many cents from everyone who receives this e-mail. Please send it to your 10 nearest friends." That thing floated around within the whole infrastructure of the country, and didn't cause too much trouble, but it struck a sympathetic chord at Scott Air Force Base, and everyone sent 10 copies to their friends. Within 30 minutes, millions of copies of the letter completely shut down all the information systems on the base. They had a very complex security system with lots of guards, but the weak point was the people's sympathy for the little girl.

Alberts: There are other stories like that. There was one, I think it was with a beeper, where they had a problem with one of the codes, and they assigned this person a special number or something, and it also mushroomed and got out of hand. So far these events have been localized and rela-

tively harmless. The Internet's been shut down on a worm, and that's extraordinarily vulnerable. You're all aware of some of the IW attacks in *The Cuckoo's Egg*¹¹ and all that, right? You're also aware that Harvard is one of the favorite places for people to use as a way station on their way to destruction, and that's because universities are open places. They don't read your mail. They don't check your identity. Have they changed? When you log on is there now a banner that says they can monitor your activities and that they reserve the right to see what you're doing and read your stuff? No, I doubt it.

Anyway, recognizing that there's a threat topology that's not well understood, I drew this. I said, "I'm going to start with this blob (figure 23), and I'm going to try to see if I make any sense of it. What I'm going to do is try to segregate the world as a function of the seriousness and the consequences."

I segregated the threat world into three parts (figure 24). Here is all this everyday stuff, and that's what we've been talking about. It happens. It's the cost of doing business in the information age. We'll

¹¹ Clifford P. Stoll, *The Cuckoo's Egg: Inside the World of Computer Espionage*. New York: Doubleday, 1989.

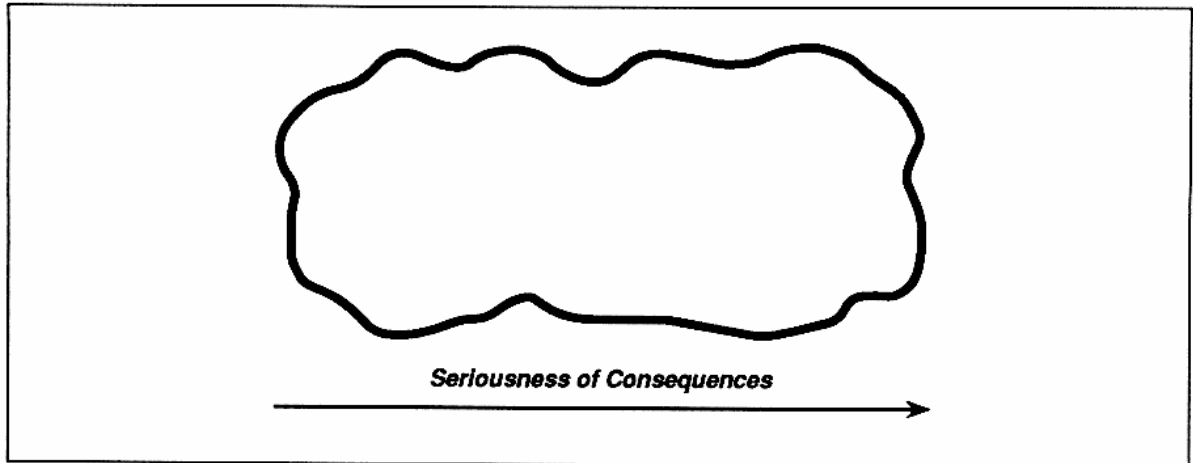


Figure 23
Threat Topology - 1

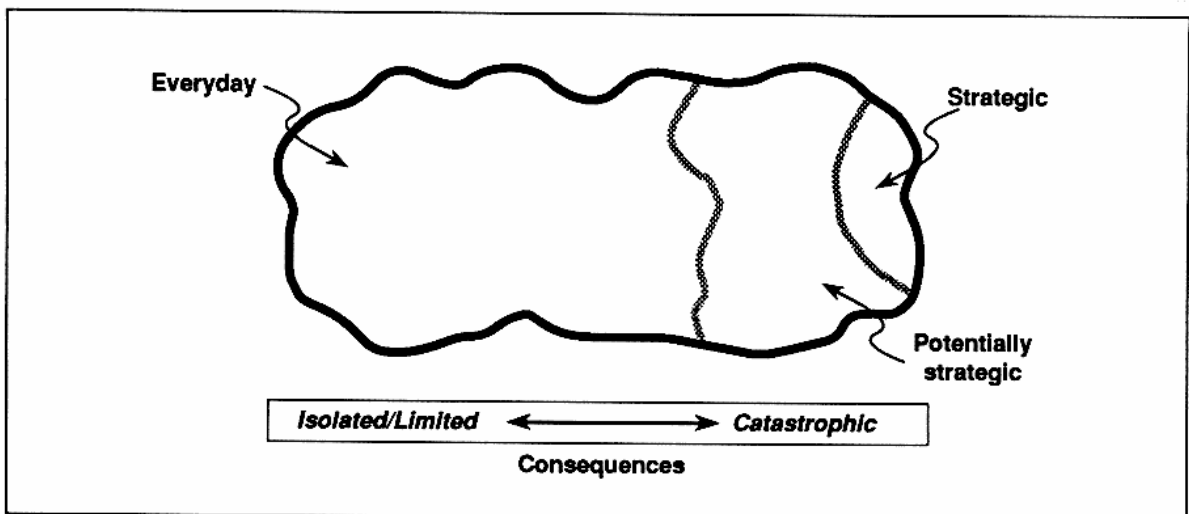


Figure 24
Threat Topology - 2

work it out. This strategic part we're also working on. We're willing to pay an enormous price here to make sure that nobody messes around with our authorizations to release nuclear weapons. No hacker is going to get into that, I can assure you. On the other hand, we're going to spend a lot of money making sure of that, and that system is going to have very limited functionality.

It's not going to do all the wonderful things that people would like it to do because it's spending all its resources on making sure that that is authenticated, accurate, robust, and reliable.

People were talking about a thing called the MEECN, the Minimum Essential Emergency Communication Network, back in 1962 when we were all afraid that the

world was coming to an end with our confrontation with the Soviet Union. But they also wanted to create something that today might be called the minimum essential NII (national information infrastructure), or something like that. That's a ludicrous idea, but people wanted to do that. The reason it's ludicrous is the same reason it was kind of crazy to have two communications systems in Russia. One quickly becomes outmoded and outdated and out of synch with what's going on in the real world, and then there's this membrane of information. We have all the good, real-time stuff over here, and then you have this other thing, which is too narrow to carry everything you want. It's very robust, but it doesn't have the functionality to do the job. So that's probably not going to happen.

In any event, there's the middle area that I'm really concerned about, which I call "potentially strategic." That's the area we don't understand at all. It's the notion that if you have three things happen accidentally in close proximity, will they cascade in such a way as to cause significant outages, loss of service, screw-ups, or economic disruption, and can that happen by some planned attack? You can conceive of an attack that hits two or three different infrastructures in ways that come together to paralyze a given area, whether it's a port that's going to send troops abroad or

something else, and does so in a way that the attack will not even be noticed by each of the individual infrastructures. Obviously, we don't understand that the real question is: Do we admit that's a possibility, and is it worth doing something, like thinking about it?

What makes this really tough is that there are lots of attacks that cut across these boundaries, and change in nature, either purposely or incidentally (figure 25). You can have a guy who started out just to be a hacker and ends up causing some real problems, or, as I said before, you have at the other end somebody who is able to orchestrate things that come together and cause problems. You have the same thing in terms of the economy. Economic warfare is perhaps really what we'll be thinking about in the 21st century.

To make matters worse, this whole thing is not a stable situation (figure 26). Every time all these people all over the world attack these systems—and this goes on every day—they're learning something. Right now, 5 percent of these attacks get noticed; at least that's what the statistics show. That means 95 percent of the time they're getting away with it, and 5 percent of the time, they know that they're either being noticed or prevented from doing it. So they're gaining information 100 percent of the time. We're only gaining information

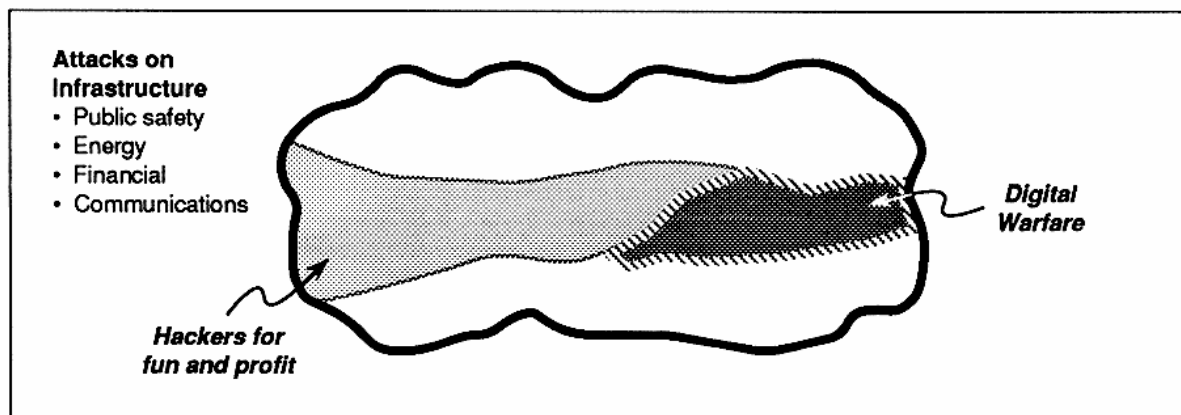


Figure 25

Threat Topology - 3

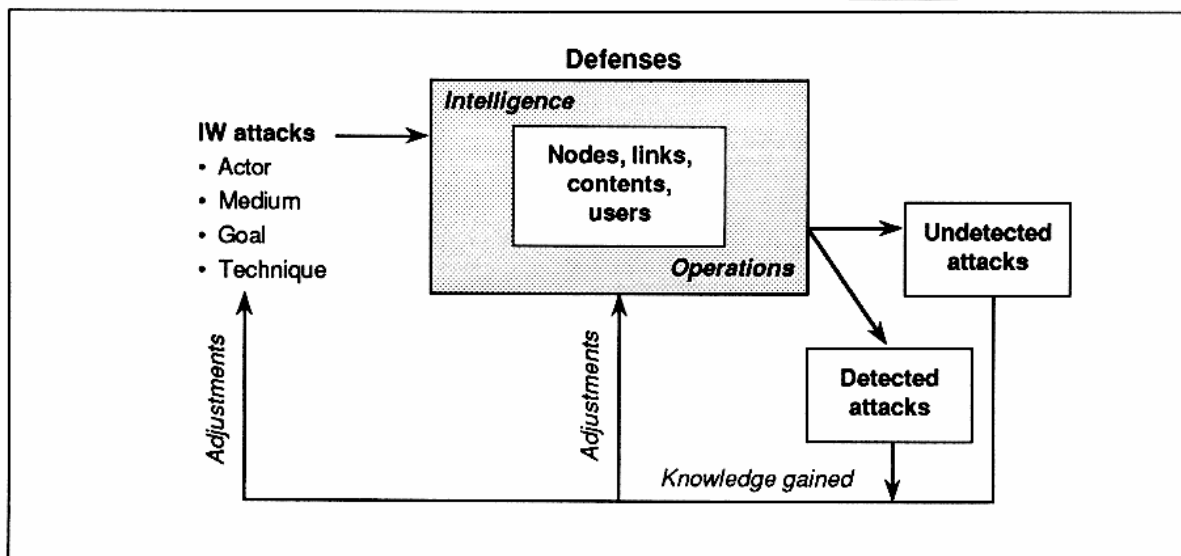


Figure 26
Threat Dynamics

5 percent of the time, so we're at a disadvantage on the defensive side. They pick the time of the attack, the place of the attack, the nature of the attack, the technique of the attack, and we're just trying to juggle stuff. Obviously, this is something that's going to be around for a long time, and inherently the offense has the edge. If the defense wants to take the edge, they do that by severely reducing the functionality of the system and hence its utility.

The problem for the intelligence community is that there is a weak mapping between organization and threat (figure 27). First of all, the source of the attack can be almost anywhere. We usually can't find that out until months later. When you get attacked, it's hard to know who it is. Second of all, even if you figure out where it's coming from, you don't really know why that person is doing it or what the connections are. So, it could be one kind of attack, or it could be another. So that's a problem.

We talked about this before: the value of the attack is a nonlinear function. A thing that only causes \$1 million worth of damage in real terms could have psychological impacts that go far beyond that and cause us all sorts of havoc in the future. If we can't rely on our ability to deploy forces, boy, that really puts a crimp in our foreign

policy! If we can't rely on the public's support for a given operation because of all sorts of things, that puts a crimp in our foreign policy. If we can't ensure that our intellectual property is protected, that creates all sorts of problems.

The really interesting thing is when you're young, you learn that you solve problems by identifying the objective functions, the uncontrollable variables, and the controllable variables, and then you concentrate on manipulating the controllable variables. Well, all of the things we want to

- **Weak threat/organizational mapping**
- **Value is a nonlinear function of outcome.**
- **Key variables are either uncontrollable or only partially controllable (e.g., technology).**
- **Trends in system design and acquisition are exacerbating the problem.**

Figure 27
IW-D Considerations

control are not in our control. That creates problems, and every trend that we notice in system design and acquisition works against us. I'll just talk about that a little bit, and then, given the time, I think I will move to another subject.

More information and more access everywhere is a good thing (figure 28). It helps us do our jobs better and be more effective. A counter to that is it makes us more vulnerable. If we separate information flow from the chain of command, we've got real problems. How do we know what's happened? How do we know it's accurate?

- **Current Trends**
 - Increased amounts of information and access provided
 - Separation of information flows from chain of command
 - Emphasis on reach-back
 - Fused and synthesized presentations
 - Increased reliance on COTS

Figure 28
System Design and Acquisition

There's an emphasis on reach-back—the concept that we in the field can go back anywhere in the world in this global grid of information and get the information we need. How the hell do we know that it's really coming from where we thought it was, and again, whether it's really valid?

We talked about fused presentations.

COTS (commercial off-the-shelf [technology]) is an example of buying critical defense stuff built by people we don't even know. We don't even know what's in it. I can assure you that in every COTS program there are things that only the developers know, because they need to be able to do maintenance on these things and test things out. There's no way for us even to test the stuff today, or to ensure that there is nothing in there that would be of concern to us.

Just one more thing on this subject: this is going to be around a long, long time (figure 29). I would bet that in 20 years people are still going to be talking about this, just the way they're still going to be talking about drugs and crime and disease. So, we're going to learn to live with it. We're going to make adjustments. We're going to pay some price, but our behavior is going to evolve until there is a balance among all of those. But that's going to take time, and you certainly don't want to be on the wrong end of that.

- **Defending against information attacks will resemble efforts to combat disease, drugs, and crime.**
 - Solution requires broad-based involvement and collaboration
 - Likely to be under-resourced
 - Interactive cycles of advances in offense/defense
 - Crises will wax and wane
 - Adjustments made to accommodate levels of "pain"
 - Natural tensions (e.g., enforcement, civil liberties)
- **A perfect defense is unattainable. There will be "leakage."**
 - This analogy extends far beyond digital war to other forms of information age "warfare," e.g., biological, chemical, environmental.

Figure 29
Analogies and Realities

Let me move right ahead. I have an approach laid out in the *Defensive Information Warfare*¹² book that talks about the nature of the problem being both a private sector and a public sector one, so there are the differences of perspectives. There's the issue that this is not a national security problem alone. We in the national security community don't have the tools actually to fix this problem without the cooperation of the private sector, or even without interna-

¹² See note 3.

tional cooperation. So it's a whole bunch of interesting challenges.

In the next five minutes, I just want to take a look at what the information age has to say for the Defense Department (figure 30). If I had to pick one thing that I would like to see the Defense Department become, it's agile. And if there's one thing it's not, it's agile. There's a lot of work to be done.

- In the final analysis, success in the information age will go to the agile.
- Transforming DOD into an agile information age organization involves:
 - An information age vision and mindset
 - Moving beyond past successes and embracing the challenges inherent in the new faces of war
 - Meeting the challenges of change
 - A new basis for long-range planning

Figure 30
An Information Age DOD

I won't mention names, but I was at a meeting where somebody was giving a talk about new forms of organization in the private sector and the information age. He said, "If a corporation is not able to make a major change in its strategic objectives in three months or less, it will be out of business." A ranking DOD official said, "I guess we're going to be out of business." Another DOD official said, "But it will be a decade before we realize it." There is some truth in that.

I think one of you guys is off to a consulting firm that's going to be helping organizations in their strategic planning and things like that, and I'm sure that one of the subjects that organizations are going to focus on is: "We can't predict the future; nobody can. But we might be able to recognize it as it unfolds before our very eyes, and if we can, maybe we can organize ourselves and have our personnel development, training, and culture be such that we can be agile and adapt to the changes."

In a book that's coming out next month on complexity, national security, and global politics (or the other way around) there is a piece by Maxfield that came out of a conference I sponsored in November.¹³ The two of us spent a lot of time talking about what you need to do to make organizations agile. When you think of all the things you need to do, and you think of government bureaucracies, you realize that it's really a daunting task. It's going to take people like you actually to do it. Within the organization you have to sort of come to some self-recognition that business as usual is not going to happen, and somehow work that through. That's the notion of the right mindset.

There are things that institutionally inhibit us from doing this. The whole notion, of course, is to start to concentrate on information as the most valuable resource that you have.

Student: Not human beings; information?

Alberts: Information is obviously useless without people. The human's ability to understand and process that stuff is what you're supposed to foster, and that's how you empower the organization. You don't necessarily do it with tanks and planes and guns and things like that. You give them the freedom to do what makes sense. That's number one. There are never any perfect things.

But basically, you're focusing attention on information (figure 30). If you think about the world, basically you have sensors, and you have what we call shooters in the military. These are the guys who make it happen, whether they're the people on the trading floor of the stock exchange, or the people producing the cars in factories, or whatnot. These are the people who are engaged in actually turning resources into products. In the "sensors" category are the people who recognize what products need

¹³ David S. Alberts and Thomas J. Czerwinski, eds., *Complexity, Global Politics, and National Security*. Washington, DC: National Defense University Press, 1997.

to be produced, where they need to go, and what the resources are.

The link between those two is really the critical one. What these sensors people are doing is taking the information and sorting through it and putting it in a form so that these shooters guys can use it. If you take the example that in World War II it took 9,000 bombs to take out a 100-foot-square building, and by the time we got to Desert Storm it took one bomb, the only real difference between that one bomb and the 9,000 is information. That's why I said that we need to focus our attention on information.

We've had these discussions. The last one I had was about where quality of life comes into all this. To me, quality of life depends on having a job that you can actually do and being given the tools that you need to do it. Of course, getting paid also helps.

This chart says more about agility, and sort of talks about the institutional barriers (figure 31). You can either feed somebody or teach him how to grow his own food, and the same thing is true in this institutional frame. I can come up with the answer for the next 5 years; if I'm really brilliant, the next 10 years (I'm not saying I know how to do this); but if I taught the organization how to be agile, then I will have done something that will hopefully last them forever.

The way to do that in a huge bureaucracy like DOD is to identify those barriers to change and break them down, and let the people who live in that organization, who will occupy it in succeeding generations, have more and more opportunity to do what makes sense. That's the way I see it.

Oettinger: Before you take it away, MTR/RMA ... ?

Alberts: The MTR (actually I believe the Russians coined that) is the military technical revolution, and that's really what we had in Desert Storm. That was not an RMA, by any stretch of the imagination. RMA is Revolution in Military Affairs, and it presumes that you actually change the

- **Point prediction in the information age will be a fool's game due to increased complexity and chaotic behaviors.**
 - Developing the ability to accommodate change and the expected will more than compensate for losses in predictability.
- **Institutional barriers must be removed for DOD to deal with change successfully.**
 - Permit the current MTR of combat to become a full RMA (perfection of traditional combat)
 - Allow DOD to meet the challenges of the new faces of war (RSA)
- **Unintended consequences always accompany change.**
 - DOD must avoid pitfalls and seize the opportunities.

Figure 31

Meeting the Challenges of Change

way you do business.¹⁴ Then there's a thing called revolution in security affairs (RSA), which says that you really have a fundamental change: the armies of the past are gone, and we're worried about all these other things. We're worried about electrons. We're not worried about tanks.

So, with that, I'll take any question on any subject for the next six minutes. I wanted to give you a chance to sort of have a dialogue.

Oettinger: What do you ask of an encyclopedia?

Student: Can you just help me understand the different systems of infrastructure? You said "power system" and "strategic system." Can you elaborate on that?

Alberts: The infrastructures that the presidential commission is working on—and this isn't necessarily in their words, but in mine—are that you have the power grid,

¹⁴ See Colonel Allard's presentation in this volume.

electricity. You have energy, which is oil and gas pipelines. You have emergency services, which are basically, I think, defined as police, fire, rescue, those kinds of things. You have transportation: railways, airlines, mass transit, highways. You have information infrastructure and telecommunications infrastructure. The news media and all that kind of get thrown in. These are the things that a society provides as a sort of fundamental foundation upon which other activities—life, liberty, and the pursuit of happiness—take place. I forgot to mention the financial institutions: banks and stock exchange and commodity exchange and all that kind of stuff. It's always easy to forget one or more of those. But the commission is looking at them.

Oettinger: For those of you who are interested, that Executive Order 13010 is not classified. You can reach it through the White House.

Alberts: I'm sure they have a home page.

Student: Yes, it's www.pccip.gov. They're actually holding public meetings, and the public meeting for the commission in Boston is on the sixth of June.

Alberts: There you go. There are 10 commissioners, one from each of many different government agencies. They have 10 whom they're getting or have gotten now from the private sector. People give up their job at AT&T or some other organization and sit on this thing for a year.

It will be interesting. Obviously, they're not going to solve the problem, but I think they're going to try to get a handle on a consensus view of the nature of the problem and recommend some government mechanisms and some relationships between the public and private sectors to work together to sort this thing out.

Student: I have another question. You had mentioned earlier that the information systems that are currently in place are very vulnerable to information attacks, and 95 percent of those will go undetected. Isn't that kind of overstating it a bit? I think that the percentage of detection has a lot to do

with the severity of the attack. Attacks that are very severe tend to get a lot of immediate attention from systems administrators and so on. For example, the Internet Worm of 1988 was a denial of service attack. You couldn't use your service, and Internet service administrators called each other across the country and were able to get things contained within a reasonable amount of time. It wasn't as though it proliferated unstoppably.

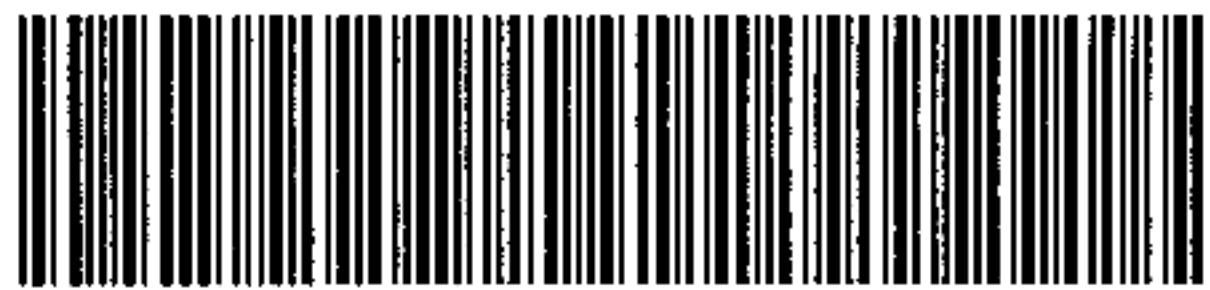
Alberts: You're right. There is the nature of the attack. Many attacks that would have significant national security implications are not denial of service or destruction attacks. They're compromise of information attacks, and those are the most difficult to ascertain. How do you know someone looked at your data? Unless it is really obvious, how do you know that someone didn't change it? That change might affect something that you don't know until much later, and then how do you trace it back to that information attack?

So, on the one hand, you're right. It's a function of the nature of the attack. On the other hand, there are probing attacks where people are trying to learn what they can do and what they can't do in preparation for a real attack, and if those are not detected, then you don't have any warning. Statistics show that if you go out and red-team another system, if you're anywhere near good, they're not even going to know it. That's a scary thing, because if we can do it, certainly other people can do it. The idea that somehow we're more technologically advanced and sophisticated than everybody in the world is sort of a nice notion, I guess, but given the nature of this educational institution and all the others, it seems to me that everybody's got access to a lot of bright people.

Willie Sutton once said, when asked why he robs banks, "That's where the money is." Information is where national security is going to be. It's not there yet, but in the next X years, that's where it's going to be. If I know that, then I'm interested in doing something about it before it's too late. It would be nice if we thought this thing through, and were prepared for this.

Oettinger: On that note, we are grateful for your timely warning, and lest we make you too late for your airplane, we now thank you. We have for you a small token of our large appreciation. We really appreciate your coming.

Alberts: Thank you very much. I will treasure this.



INCSEMINARS1997



ISBN-1-879716-47-X