INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Asymmetric Approaches to Joint Vision 2020
Thomas R. Wilson

Guest Presentations, Spring 2001
C. Kenneth Allard, Cheryl J. Roby, Nicholas Rostow, Richard P. O'Neill, Harry D. Raduege, Jr., Thomas S. Moorman, Jr., Thomas R. Wilson, James M. Simon, Jr., Toshi Yoshihara

November 2001

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

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

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-76-3 **I-01-3**

November 2001

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

Anonymous Startup
AT&T Corp.
Australian Telecommunications Users Group
BellSouth Corp.
The Boeing Company
Booz•Allen & Hamilton, Inc.
Center for Excellence in Education
CIRCIT at RMIT (Australia)
Commission of the European Communities
Critical Path
CyraCom International
DACOM (Korea)
ETRI (Korea)
Fujitsu Research Institute (Japan)
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
Hitachi Research Institute (Japan)
IBM Corp.
Korea Telecom
Lee Enterprises, Inc.
Lexis–Nexis
John and Mary R. Markle Foundation
Microsoft Corp.
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
NEC Corp. (Japan)
NEST–Boston
Nippon Telegraph & Telephone Corp (Japan)
PDS Consulting
PetaData Holdings, Inc.
Research Institute of Telecommunications and Economics (Japan)
Samara Associates
Sonexis
Strategy Assistance Services
United States Government:
- Department of Commerce
  - National Telecommunications and Information Administration
- Department of Defense
  - National Defense University
- Department of Health and Human Services
  - National Library of Medicine
- Department of the Treasury
  - Office of the Comptroller of the Currency
- Federal Communications Commission
- National Security Agency
- United States Postal Service

Upoc
Verizon

Asymmetric Approaches to Joint Vision 2020

Thomas R. Wilson

May 3, 2001

Vice Admiral Thomas R. Wilson became the thirteenth director of the Defense Intelligence Agency [DIA] in July 1999. As director, he manages the General Defense Intelligence Program [GDIP], overseeing selected intelligence resources for all services as part of the National Foreign Intelligence Program. Following early assignments in the United States and abroad, he served as the fleet intelligence officer and assistant chief of staff for intelligence, U.S. Seventh Fleet (June 1987–July 1989). Returning to Washington, D.C., he served as the special assistant for intelligence to the deputy chief of naval operations for naval warfare. He became director of fleet intelligence, U.S. Atlantic Fleet, in April 1991 and served as the director of intelligence, U.S. Atlantic Command (April 1992–November 1994). He was promoted to flag rank during that assignment. Subsequent flag assignments include vice director for intelligence on the Joint Staff, associate director of central intelligence for military support, and, most recent, director for intelligence on the Joint Staff. In addition to campaign and unit awards, his personal awards include the Defense Distinguished Service Medal (two awards), Defense Superior Service Medal, Legion of Merit (two awards), Meritorious Service Medal (two awards), Joint Service Commendation Medal (two awards), and the Navy Commendation Medal (two awards). He is also the recipient of the Director of Central Intelligence and Defense Intelligence Agency Director's awards. He was graduated from the Ohio State University with a B.S. degree in agriculture and earned an M.S. in management and human relations from Webster College. He was also graduated with distinction from the Defense Intelligence College.

Oettinger: I take great pleasure in introducing our guest today, Vice Admiral Thomas Wilson. I won't make a long introduction, because you've all had a chance to read his biography. He has indicated that he is amenable to questions as he goes along, so go right ahead. It's all yours.

Wilson: Thanks very much, Tony. It's great to be here. I've been in Boston before, but I've never been at the Kennedy School or at Harvard. As you may know, I actually have a college at the DIA: the Joint Military Intelligence College [JMIC], which gives bachelor of science and master of science degrees in strategic intelligence. Tony is the chairman of our board of visitors. He is a great supporter of our college and does tremendous work for the DIA.

I don't exactly know how a guy like me should feel being here, with Harvard's age and reputation for academic excellence and things like that. My degree is in agriculture from Ohio State (you may have seen that), so I hope I'm not too intimidated by being here at Harvard.

I have absolutely no imperative to give you this prepared brief if you'd prefer to do something else. It won't take too long in any case, and I'll be happy to go wherever you would like in this class with regard to what you know about me as director of the DIA. I just brought this briefing along as a way of perhaps letting you know how we addressed some issues with the Congress this year about asymmetric threats and asymmetric warfare.

Every year, the Congress kicks off its legislative year with a series of worldwide threat hearings. The director of central intelligence [DCI], George Tenet, and I testify before a number of committees: the House and Senate intelligence committees, the House and Senate appropriations committees, and the House and Senate defense committees. It's usually a three- or four-hour session in which they try to challenge our bladder control as they go in and out and get their coffee and we're stuck there. George Tenet does a tour de force around the world and talks about the worldwide threat. You can imagine what the subjects would have been this year: information warfare, terrorism, the Middle East, Korea, China, Taiwan, et cetera. I decided to take a slightly different approach, because in the past we just covered the same ground from a different perspective. I decided to address our joint vision in the military and the asymmetric threats or asymmetric approaches that countries can take to attack it.

We all know what "asymmetric" and "asymmetry" mean, and we all are aware of terrorist and other kinds of events that occur against the military or even against our homeland. The different twist, or the new way that we're trying to look at this, is specifically as a counter to our military vision, our military strategy, and our military doctrine of the future. The reason we try to do this is that the Department of Defense [DOD] has a *Joint Vision 2020* Web site (you may have visited it),[1] and there are more foreign hits on that than on any other single Web site in the DOD. Some would choose to believe that the joint vision is so overpoweringly dramatic that everybody wants to learn from it, but I am the nation's senior military intelligence officer and I choose to believe that a lot of people are out there trying to learn how to defeat it. I'd like to talk for just a few minutes about that. You can ask questions on the way, and then we can get into a range of issues afterwards.

We know through a lot of intelligence and even open sources that our adversaries, or would-be adversaries, recognize current U.S. strength, particularly military strength (**Figure 1**). Countries such as China have intently studied, for example, the results of Desert Storm—the war in the Persian Gulf that concluded in 1991—and then they've seen what happened in Desert Fox against Iraq in 1998 and in Allied Force—the precision strikes in Yugoslavia. Many of these adversaries have concluded that they can't and don't even want to try to fight us force-on-force, head-on, in a conventional military war. They want to avoid conflict on those terms, which would be our terms, and if they have to have a conflict with the United States, or maybe even NATO [North Atlantic Treaty Organization], they want to have it on their terms.

Take a look at the four tenets of *Joint Vision 2020* for the future (the first four bullets on the right of the slide). God only knows—we have a new administration, and they may trash

---

[1]Chairman of the Joint Chiefs of Staff, *Joint Vision 2020* (Washington, D.C.: U.S. Gov't. Printing Office, June 2000), [On-line]. URL: http://www.dtic.mil/jv2020/jvpub2.htm (Accessed on October 24, 2001.)

Figure 1

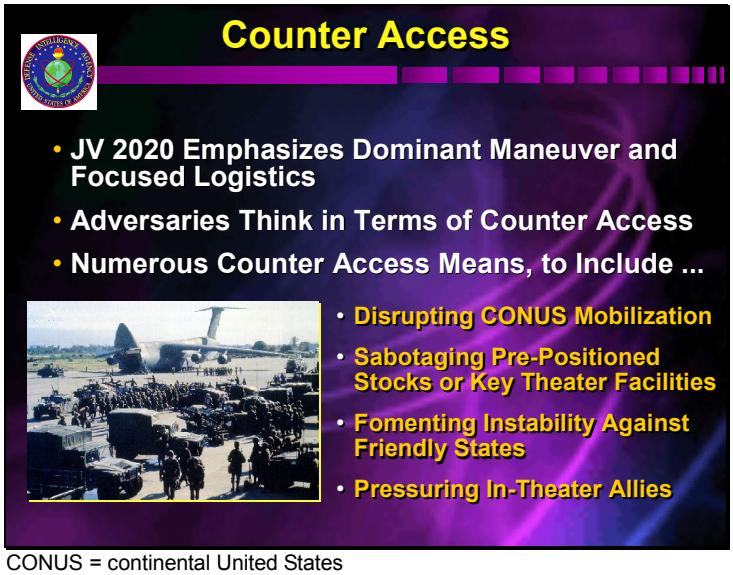
Joint Vision 2020, and we may be off on a new vision, but I suspect some of these tenets are pretty perpetual. Dominant maneuver is the ability to move your force to the battle or on the battlefield if you need to. We need the ability to support the force with on-time logistics and supply. We certainly need to try to capitalize on our ability to use precision engagement as opposed to mass firepower, carpet bombing, or things like that.

The fourth bullet is really important. We have got into an age where full-dimensional protection is critical. It is very difficult to engage in what I would call a political war or political conflict—the kind we were engaged in during the late 1990s, such as Bosnia and Kosovo—and not have any losses. This has to do with how you protect your country and your deployed military, and it has a lot to do with national missile defense, theater missile defense, protection against terrorism, et cetera.

These four tenets are supposed to be enabled by information superiority. Information superiority, in my view, has a very simple definition: it means you know more about your enemy than the enemy knows about you. It's a kind of net assessment.

Not in *Joint Vision 2020*, but critically important for our military, is something called national will: Do the citizens of the country support what the political leadership wants to do with their sons and daughters who are in the military? I want to discuss how the thoughts in the upper left of the slide interact with the thoughts at the lower right.

Dominant maneuver and focused logistics have everything to do with getting our force to the battlefield and being able to use it on the battlefield (**Figure 2**). We think in those terms. Our adversaries think in terms of counter access and how they can prevent this dominant military force from getting in or even to the battle. There are a lot of counter access means that in the past we often tended to ignore in our war planning. For example, disrupting our ability to generate reserves, or military force, in the continental United States has never even been threatened in any war we've had. Sabotaging our key ports or airfields of entry in theater by attacking them as we deploy or before we deploy also has not occurred. We in the DIA also believe that no adversary



CONUS = continental United States

Figure 2

is likely to repeat what Saddam Hussein did, which is watch the U.S. military build up for six months in Saudi Arabia and the Gulf region to project power against Iraq. Future adversaries could try fomenting instability against friendly states that might politically or logistically support a military deployment, or pressuring in-theater allies. Dominant maneuver and focused logistics are key tenets of *Joint Vision 2020*, so, if you're a military force or a country that wants to oppose the United States, your dominant tenet might be counter access.

I'd like to talk about counter access in several ways. Here are a couple of Navy examples (in fact, there are a lot of Navy examples). This is a Russian missile, the SS-N-22 Sunburn, which is being sold to India and to China (**Figure 3**). These missiles are on the Russian ships that went

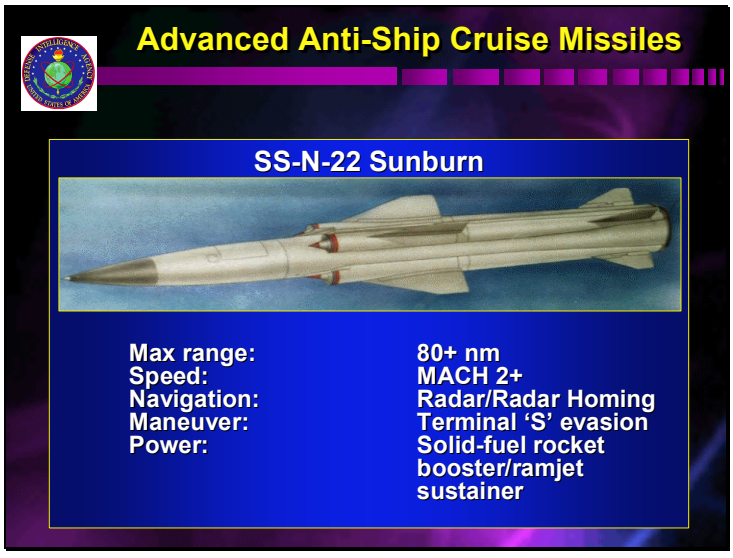
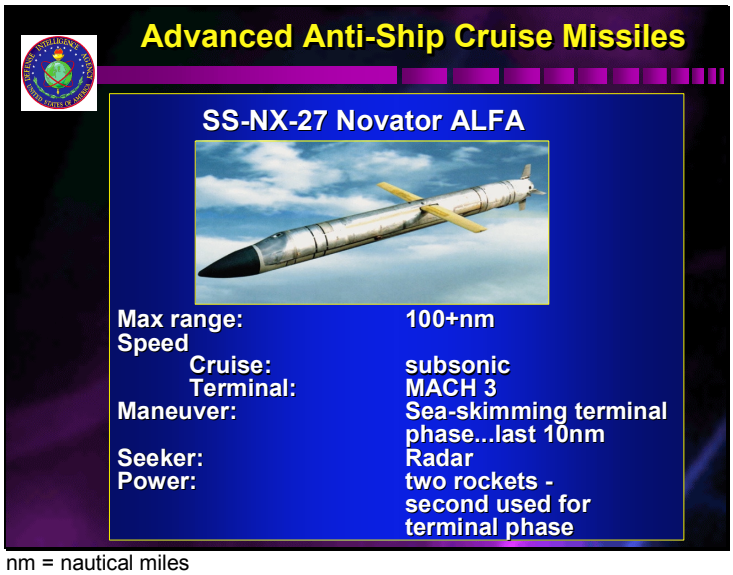


Figure 3

to China: the Sovremenny-class destroyers. They are very capable missiles. They have never been used in combat, but could be used against the U.S. Navy or, even more easily, against supply ships—maritime pre-positioning ships—that are trying to bring capability into a theater.

An even more powerful and more difficult modern missile is the SS-NX-27 (**Figure 4**). The Russians don't even field this in their own force. It is not operationally deployed in the Russian navy, but has already been sold to the Indian navy and, we believe, is going to be sold to the Chinese navy. So here's a country, Russia, whose main goal is trying to maintain an economic base, selling modern cruise missiles to adversaries who, we believe, would use them primarily for counter access—to prevent us from having access to a theater.



nm = nautical miles

Figure 4

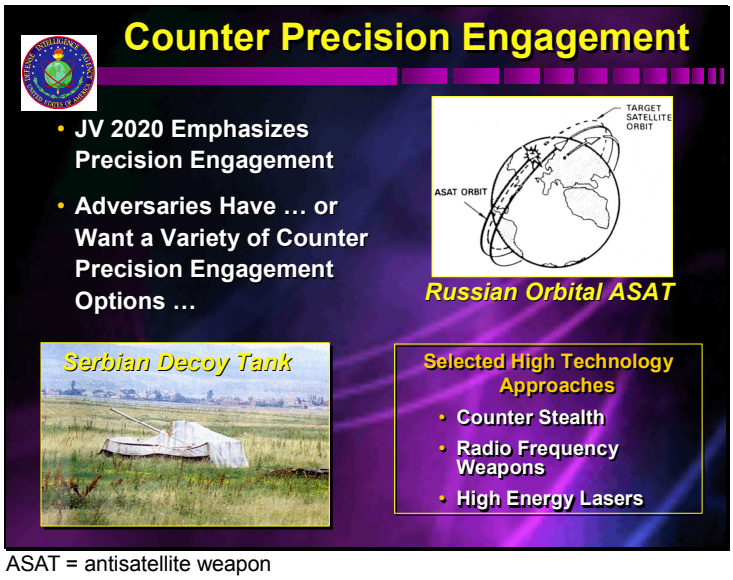
There are a lot of things that enemies can use besides missiles (**Figure 5**). One of the key areas we're concerned about in terms of counter access is the Persian Gulf. We operated there with relative impunity during the Gulf War. We had three aircraft carriers maneuvering in that very small body of water, and three more in the Red Sea, flowing supplies and troops to Kuwait and Saudi Arabia through the Straits of Hormuz. Iraq could do nothing about it.

Iran has watched that. Iran doesn't want us to be able to flow things into the Persian Gulf. So we have Iranian swarm tactics, shown at the upper left of the slide. We may be able to defeat another aircraft carrier battle group, or a submarine or two, or an opposing naval force, but how, exactly, does the U.S. Navy defeat a hundred boats with some kinds of standoff missiles or machine guns that are swarming around like bees, especially if ten of the hundred are suicide bomber boats. It's not just our navy that's at risk; it's the other ships.

The bottom left of the slide shows the kinds of missiles that ring the Straits of Hormuz. They can lay down a cover of fire against naval forces. Old World War II contact mines, deployed indiscriminately, can prevent access, and, of course, there is even more modern equipment, such as Kilo submarines.

Figure 5

The leadership of our country has been enormously fascinated with precision engagement for a decade or more, because it does several things (**Figure 6**): it allows you to hit targets precisely and to limit collateral damage. We certainly have problems now and then—even precision weapons don't always hit their targets. Our adversaries are now trying to determine their best ways of countering precision engagement, not because they could necessarily defeat us militarily, but because, by causing collateral damage, by not allowing us to hit targets that count efficiently, effectively, and quickly, they can erode our national will.



ASAT = antisatellite weapon

Figure 6

Again, there are all sorts of ways to counter precision engagement, from the very low tech (decoy tanks that make you waste your precision weapons, which cost five, ten, or fifteen times more than nonprecision weapons) to more advanced things, such as orbital antisatellite capability,

which tries to deny us our precision intelligence, surveillance, and reconnaissance. To be able to attack things precisely with weapons is one thing; you also need precise information about what you're attacking, where it is located on the face of the earth, and how you can attack it. In addition to the low-technology things, adversaries want to be able to use counter stealth technology to interfere with our precision weapons, and radio frequency weapons to counter such assets as our Global Positioning System [GPS], which allows us to navigate precisely anywhere on the earth. They also want to employ ground-based, high-energy lasers against GPS and other targets. These are all high-technology approaches coupled with low-technology approaches that are aimed at denying us the ability to use our precision weapons.

Some of them are pretty simple. There are about 10,000 deep underground facilities in the world (**Figure 7**). Countries are learning the value of going deep underground, because, even if you have the technical capability to penetrate through meters of rock and soil, you cannot necessarily know exactly where the target is that you want to hit and exactly how to attack it. We had an interesting example of this in Kosovo. On another occasion, down in Montenegro, we were better.

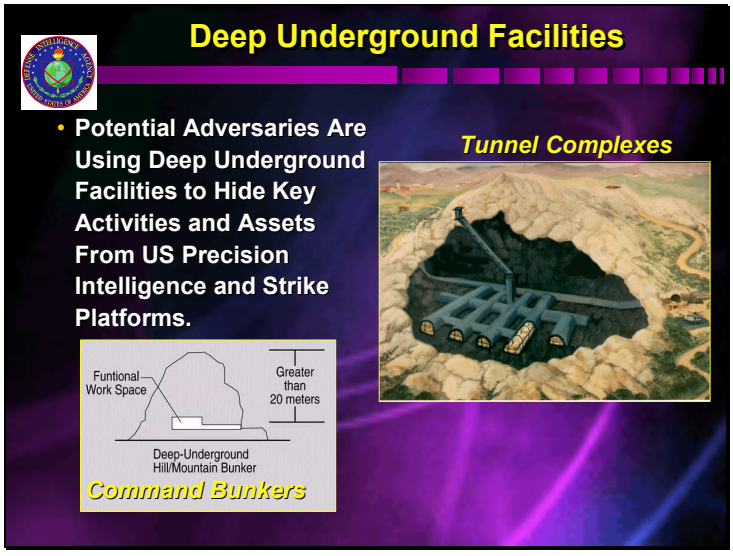


Figure 7

Student: The Taiwanese also have facilities like this, if I'm not mistaken. As we try to learn how to knock out other people's facilities like that, are we doing anything to help people, including ourselves, who have facilities like this to learn how to mask them better?

Wilson: We certainly approach it in a number of ways. We've built our own underground facilities for a long time, mostly because we were concerned about nuclear warfare in the cold war. In terms of how you build them, first of all, we now have advanced mining and engineering techniques, where huge bores or drills can go through mountains. The ability to build deep underground facilities is much greater than it was fifteen or twenty years ago. We use engineers to look at how to use geology to construct them, and we use other kinds of intelligence mechanisms to determine precisely how certain countries build certain facilities. An approach we can use is to study individual suspect areas with traditional intelligence sources, as well as learn through open

source literature and contract our own expertise to understand from an engineering perspective exactly how we or somebody else builds these facilities.

Student: I'm glad you brought up open sources, because I was going to ask you about that. Within the DIA, is there a dedicated OSINT—open source intelligence—directorate or shop, or is it integrated into functional and regional areas as just one of the disciplines in multidisciplinary intelligence?

Wilson: Both. We have a modest directed open source effort, and most analysts and analytical groups routinely incorporate open source at the desktop to supplement their classified holdings. But it's like everything else: every advantage is also a potential disadvantage. If you want all analysts to have open source Internet access at their desks, do you want them to have it on the same computer as their classified Intelink intranet access? What are the implications for information security and protection? You're the director of the DIA, you have 7,000 people working for you, and you need to double the number of workstations you have. There are a lot of issues as to how best to administer an open source program in conjunction with the classified research and analysis that's going on. We're using open sources more and more, and we have both the modest open source effort as well as strong encouragement to incorporate open source information in the regular workplace.

Oettinger: I'm puzzled as to why you labeled what you're describing for us as "asymmetric." Let me try to clarify that. A terrorist attack on Khobar Towers or on the World Trade Center or on the Murrah Building is a sort of asymmetric, David-and-Goliath undertaking, but on the other hand, except for the victims directly affected, it does not accomplish a hell of a lot, whereas what you're describing here are activities essentially meant to deny the effectiveness of a whole force. In every example, I think to myself, "If I really wanted to pull this off, even that swarm of boats, I would need a fair amount of intelligence, I would need a fair amount of preparation, I would need a lot of other things," so it doesn't look all that asymmetric to me. It looks like a fairly substantial force preparation, whose presence and mustering and so forth would require a lot of resources, and therefore would be vulnerable in a way that "asymmetric" and terrorist things are not.

Wilson: I think there are a couple of things about all of them that put them in the asymmetric category. One or two hundred cigarette boats are asymmetric in cost. In other words, for example, we project power with a carrier battle group that represents an investment of $25 billion. They try to counter it with an asymmetric strategy that represents hundreds of thousands of dollars, or even less.

A command bunker is, in one view, a traditional way to protect something that's of value to you, but it's asymmetric if the cost is too high to us. It's probably asymmetric because of the kinds of wars or engagements we find ourselves in. It becomes less asymmetric if you're in a full-up Korean War, where there's a traditional battlefield and a traditional demilitarized zone, with the bad guys on one side and the good guys on the other. Here, it's how much effort you have to expend, and how much national will and how many resources you have to use up to accomplish your national goals. I guess the way I would say it is that many things can be both asymmetric and very traditional.

This next slide just talks about decoys, deception, and relatively low-cost ways to achieve disproportionate results (**Figure 8**). It shows Serbia's attempt to make something look like a real

Figure 8

bridge as opposed to what it is: a fake. Sometimes disproportionate results force us to expend expensive and treasured precision munitions on bad targets, or force us to expend them in areas where they cause disproportionate collateral damage, which I'm going to talk about in a few minutes.

Human shields are one of the real asymmetric tactics (**Figure 9**). Saddam Hussein puts children in front of palaces and command and control centers so that we either will not attack them, or, if we do, we will create collateral damage that is unacceptable to our leadership, our people, and our allies.

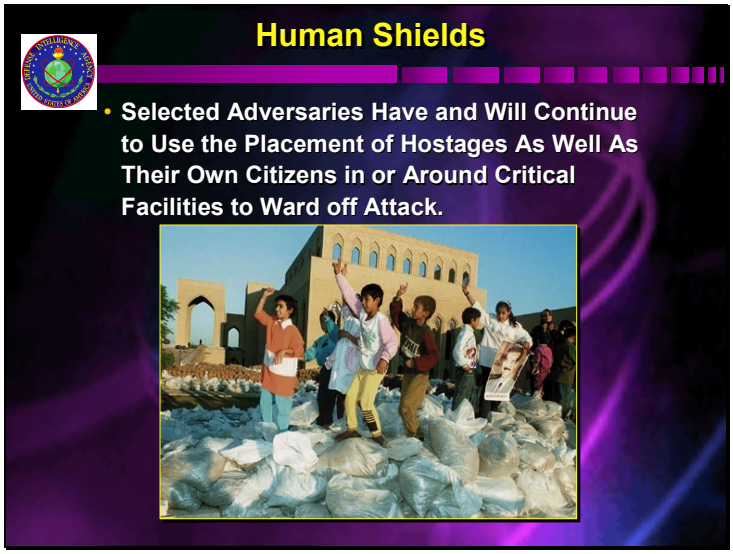


Figure 9

Counter protection is another issue (**Figure 10**). We think that the *Joint Vision 2020* concept of full-dimensional protection is important, whether it's against terrorism, or proliferation of

Figure 10

weapons of mass destruction [WMD], or new kinds of conventional weapons that most people don't know much about, such as volumetric munitions. Counter protection has to do with the ability to inflict damage on us in a disproportionate or asymmetric way—disproportionate in cost.

Volumetric weapons are a good example (**Figure 11**). We hear a lot about chemical weapons, biological weapons, and nuclear weapons, but volumetric munitions are much cheaper, much easier to manufacture (they don't rely on any dramatically advanced technology), and widely available from proliferant countries, such as China and Russia, or at arms markets and international arms expositions. Essentially, they mean using conventional explosives in a different way. This graphic compares the effects of conventional high explosives to those of volumetric

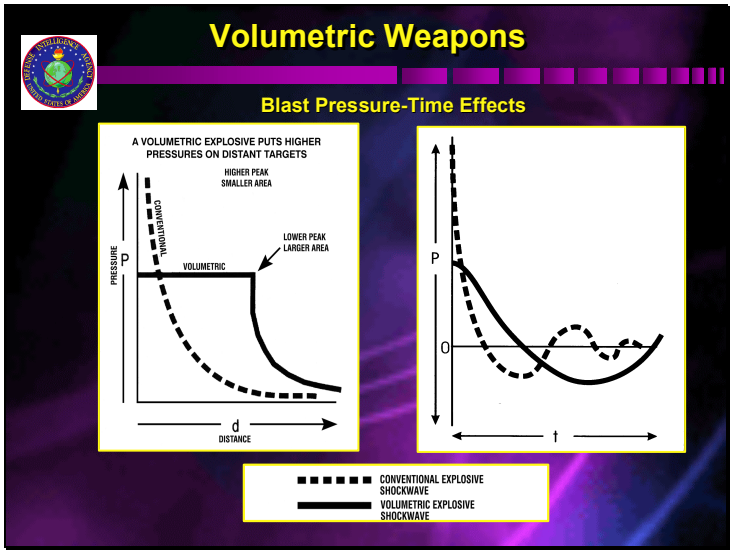


Figure 11

weapons in terms of the overpressure[2] produced (the vertical axis) and distance from the detonation (the horizontal axis). As you can see, the real effect of volumetric weapons is that they produce and sustain higher levels of pressure over much greater distances and for longer periods of time.

The challenge, or problem, with volumetric munitions is that they defeat conventional protective mechanisms. For example, if soldiers are wearing body armor designed to protect them from shrapnel, volumetric munitions will cause damage to their internal organs that will not even be visible on the outside. In the kinds of medical treatment that we use on the battlefield, the first two things we try to do for soldiers injured in battle is to hydrate them—put them on intravenous fluids—and evacuate them by air once they're stabilized. Both would be exactly the wrong things to do if volumetric munitions were used, because hydration will essentially cause internal drowning, and the pressure associated with air evacuation will exacerbate internal injuries. Do your tank hatches work? Do your foxholes work? These are classes of weapons that are of great concern to us. I can say to you that if Timothy McVeigh had used a volumetric weapon of the same size as the bomb he used in the Oklahoma City bombing, there would have been an estimated twenty times the casualties, so it's a dramatic difference.

Student: I'm not very familiar with volumetric munitions. Are they easy to get? Are they difficult to produce?

Wilson: They are fairly easy to get. They are not expensive. They are not cheap, either, but the kind of adversary we're talking about can get them. The crudest form of a volumetric munition is a fuel-air explosive. Fuel-air explosives have the effect of extending the distance and the time of the blast overpressure. But there are other techniques, such as thermobaric grenades. Here's a good example. A grenade fired from a grenade launcher that hits a window at one of our embassies and goes in will cause relatively minor damage. A thermobaric grenade of the same kind will collapse the entire building and certainly have a far larger kill radius inside. The packaging of metal powders around high explosives creates the same effect.

Student: What kinds of countermeasures are out there for volumetric weapons?

Wilson: There are ways of protecting yourself, but they are different from protecting yourself against conventional munitions. They involve the ways you would manufacture shelters, or hatches on tanks, even the tactics, techniques, and procedures [TTP] our medical people would use if there were such an attack.

Here's another point I guess I haven't made as much as I should. Using volumetric weapons doesn't cross the threshold of using chemical, biological, or nuclear weapons. There is a proscription against those in terms of treaties and other formal documents, but there are no treaties against volumetric weapons. They don't have the same psychological impact as using chemical weapons, but they may have the same impact in terms of physical damage. Volumetric weapons are just an example of asymmetric approaches that represent a relatively low investment that can have an asymmetric physical or psychological impact on the targets.

Information superiority is obviously important for our country (**Figure 12**). It is a tenet of *Joint Vision 2020* that empowers the other tenets. There is a rapidly growing threat, ranging from

[2]Overpressure is pressure significantly above the usual or normal atmospheric pressure.

Figure 12

computer hackers to organized state attacks against computer systems. But there are other kinds of information superiority. Sometimes it's the quality of the information that's being put out, typically psychological warfare taken to extreme levels in terms of how sophisticated it is, destroying and disrupting the flow of command, control, and communications. Of course, the ones we think most about right now in an asymmetric or unconventional sense are computer network attack and cyberwar. Potential adversaries are developing the means to attack our key information systems, and we're most concerned about organized, widespread, sophisticated country approaches, but there are other potential sources, such as terrorists, crime syndicates, and foreign corporations.

This is a chart that some agree with and others disagree with (**Figure 13**). It's good, I guess, for the sake of discussion. It shows the level of harm that can be done, ranging from propaganda, nuisance low-level attack, espionage, and brief, isolated, disruption to widespread information damage to critical infrastructure. It also shows the kinds of perpetrators, from hackers all the way to national governments, and an estimate that was taken from an NIE [National Intelligence Estimate] about our level of concern with regard to how these groups can perpetrate anything. I think the most important thing to take away from this is that while hackers, cyber terrorists, and industrial spies can do a lot of things, we believe that the most serious threats remain organized, large-scale, national governments conducting cyberwar against us—not just espionage, not just isolated damage—that has the potential to do widespread and critical damage to the infrastructure if you can't defend against it. It is a way to introduce uncertainty into our decisionmaking process if we can't have a dependable electrical system, if we can't have a dependable transportation system, or if we have trouble even logistically in using computer networks to control shipping, airflow, and all that. If that's disrupted, how does that interrupt not only your country's infrastructure and operations but also the force flow?

Student: Admiral, is there a dedicated information warfare department within Transnational Warfare, for example, at the DIA, or does the DIA send analysts to other national intelligence agencies?

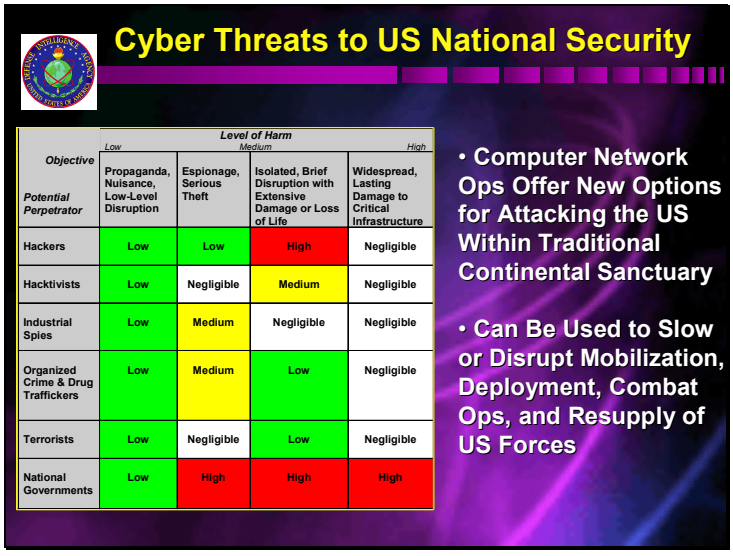


Figure 13

Wilson: As you know, U.S. Space Command has been given the mission of information operations, among the unified commands. They have a joint task force for computer network defense [JTF–CND], which is at the Defense Information Systems Agency [DISA]. General Raduege, when he was here a couple of weeks ago, probably talked about that quite a bit.[3] We actually provided the J-2—the intelligence officer—in the JTF–CND. We certainly have a group of people in the DIA who are dedicated to working this threat. So I think the answer to your question is yes. The real questions are: Are we robust enough, and how manageable is this problem? How do we scope it and prioritize the effort so that we can actually protect our really key infrastructure, and who's going to decide what's key? Is electrical power more key than banking? Is air traffic control more important than the telephone system? It's one question after another.

I don't think this is a surprise to anybody (**Figure 14**). We saw this happen before. Saddam Hussein tries to counter our will all the time by using psychological operations against his neighbors in the Gulf countries, trying to shape domestic and foreign opinion. The threat of using mass casualty weapons is designed to reduce our will to engage. So, for example, if the country is debating engagement in a new Gulf War or a defense of Taiwan scenario, and China or Iran or Iraq threatens large-scale, mass-destruction attacks, is our political will eroded?

Allowing extensive collateral damage to occur, or setting it up, is one of the methods adversaries could use. We could have lost interest in the Yugoslav operation very quickly had we had a significant collateral damage incident early. We had one where a convoy was hit, but it happened more or less midway during the war. Had it happened in the first day or two, would NATO have been able to hold together? Would leaders of countries set up scenarios to cause that type of damage to occur?

---

[3]See Harry D. Raduege, "DISA and NCS," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2001* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-01-3, September 2001), [On-line]. URL: http://www.pirp.harvard.edu/pubs/html

UNSCOM = United Nations Special Commission

Figure 14

The slide also shows the "parade of dead children" in Baghdad. It happened in the early 1990s. Of course, we think that some of the dead children were the result of Saddam's operations against the Shiites, not the result of any bombings.

Oettinger: That viewpoint about national will has become kind of a tenet of *Joint Vision 2020* and I just wonder about its solidity. Ernest May, in his book about the German invasion of France in 1940,[4] makes a persuasive case for a very rapid shift in French and English attitudes toward war, which was somewhat miscalculated. In 1938, the attitude was still very pacifist; by 1939, *boom!* There was a very abrupt flick. It seems to me that when you look, for example, at the reactions to the U.S. plane landing on Hainan, the U.S. public would have been ahead of the leadership in that one. I'm just wondering how heavily we can lean on this. It seems to be a very flimsy assumption.

Wilson: It's scenario dependent. If we're truly threatened as a country, counter will is not a very big deal, because America responds, and will always respond, when we are threatened. But in the 1990s, the military was used to pursue Haiti, Bosnia, Kosovo, and Somalia, and those operations were not robustly supported by the populace in any case. Had the adversaries been more sophisticated in their tactics or their ability to erode the will of the Congress or of the people, they could perhaps have prevented operations from occurring at all. It's those kinds of intermediate scenarios where we think counter will comes into play most heavily.

What I've really outlined are what we think are low-cost potential ways of countering *Joint Vision 2020* (**Figure 15**). Even though we may have a vastly superior military, many countries that could effectively employ one or a combination of these asymmetric tactics or strategies could potentially have a chance of success against us. If we want to have a military that can fight and win the nation's wars or chosen conflicts, a real concern for us should be whether the mere threat of these kinds of asymmetric strategies could erode our willingness to fight or deploy at all, or to

[4]Ernest R. May, *Strange Victory: Hitler's Conquest of France* (New York: Hill and Wang, 2000).

Figure 15

use the military in ways this country has used the military ever since the end of the Korean War, or certainly since the end of the Vietnam War. I think these are all important things that we have to understand from the intelligence perspective and make decisionmakers and policy people understand if they're going to pursue a joint vision for the military that actually does empower the force. There are ways of countering asymmetric advantages. They don't mean the enemy is ten feet tall, but they do mean that we probably have to consider these kinds of things more effectively than we have in the past.

That was the end of asymmetric warfare. This is the last slide (**Figure 16**). You won't be tortured any longer. I just want to set the stage a little bit for what I do, and what we do at the DIA. I'm director of the DIA, which is about a 7,000- person operation. It operates worldwide. I'm also de facto the director of military intelligence [DMI]. It's not in legislation or statute, but my job is to coordinate all of defense intelligence, which includes Army, Navy, Air Force, Marines, and the intelligence organizations of the unified command structure. For about the last eighteen months, we have been embarked on a program where we try to identify our most pressing, big-issue challenges, and I just wanted to tell you where we're concentrating our efforts, because it may stimulate questions on issues that you'd like to talk about.

My perspective is that even though our job in intelligence is to focus on the future, there are no facts about the future. We don't know for sure what's going to happen. People ask, "Will Russia ever be able to revive itself and become a global conventional competitor?" The truth is, we don't know. We don't see prospects of it in the next five or ten years because of the economic situation in Russia, but we also didn't forecast the fall of the Soviet Union. Is China going to become a world-class conventional competitor or even a world-class nuclear power? The answer to that is: we don't know for sure; however, if they spend not 5 percent but 12 percent of their gross domestic product on the military, it could make a significant difference in the equation. Why haven't terrorists used WMD up to now? Frankly, I don't know, but we estimate that there is a greater than 50 percent chance they will.

Figure 16

The Military Intelligence Board contends that the best way to focus on the future is to build on the fundamentals of our business, so the slide shows four of what we call "thrusts" that the military intelligence community is working on aggressively and where it is trying to make great progress. The first involves attacking the problem we have with worldwide databases. In the intelligence community, our tendency has always been to fuel our fascination with current and crisis events: the current war, the current deployment—everybody working hard to support the current military operation. We have gotten 35 percent smaller in the last ten years. The number of requirements has grown exponentially, and the demand that we know about the world is higher than ever, so we have a major database issue in terms of its being current, correct, collateral, interoperable, quickly [C3IQ]. You love acronyms, right?

The bombing of the Chinese embassy in Belgrade was an acutely unpleasant experience for me. I was the J-2 (the director of intelligence) on the Joint Staff, so I was the one who showed the picture of the Chinese embassy to the president of the United States (among 900 other pictures I showed him) and said, "We're going to bomb this, because it's the Yugoslav department of military procurement." We had good sources that said that's what it was; another agency (not my own) got that information and gave us that identification, and our databases were not able to find that mistake in targeting. Even though we had people in the system who knew that building was the Chinese embassy, it had not been entered into the database.

The second thrust involves intelligence integration and interoperability to achieve a common operational picture [COP]. If you have to look at a city, or a country, or the world, keeping that database current, up to date, and interoperable is a dramatic challenge, and we have really refocused our efforts on trying to do that in a three-tiered way. First, in the near term, using what we have today, which is the very flower of 1970s technology, we have an aggressive push to update information on the countries and categories that we think are most likely to concern us in the future. Second, in the mid-term, we plan to change the rules to increase our capability to update the database directly from reporters in the field, collectors, and imagery analysts, as opposed to an all-source process that can get bogged down. Third, we want to beam ourselves into the future with a Web-enabled knowledge base of hyperlinked data, which is completely

different from the fixed databases we have today. The biggest challenge we have is that we can't just stop doing what we're doing and beam ourselves into the future. We're trying to do all this on declining budgets, so we're trying hard to make what we have better even as we project ourselves into the future. This means making our stuff—intelligence—plug and play with the operators' stuff. We have a very interoperable intelligence community. We have worldwide linkages, video teleconferencing, and virtual workspaces, but we increasingly need to make sure that our SECRET compartmented stuff plugs and plays on the kind of equipment used by the warfighters in a way it hasn't before.

Fourth, we have to shape the military intelligence community to meet asymmetric threats. They include terrorism, drugs, and other things we talked about. There's a gap, because the community still has a force-on-force structure to it, a force-on-force mentality: army versus army, navy versus navy, air force versus air force. We can't junk that, because we still deploy and we still have to be prepared to fight in that mode, but increasingly the only threats to the homeland are asymmetric. As I tried to describe in the earlier part of the presentation, they are also potentially the main threats, in many countries, to our military strategy. So we have to learn how to address these threats efficiently and effectively, even as we continue with our force-on-force approach.

Further, we must revitalize and reshape our workforce. We know we're going to need new skill sets in different mixes for the future. We're not so diverse a community as we should be in terms of the ethnic and religious diversity of our workforce, especially at senior levels. I actually have 60 percent civilians in the DIA. We have to make sure we can find, recruit, train, retain, and appropriately reward the right people with the right skill sets to deal with the kinds of future threats we have. If we can't do that, we have essentially no chance of doing these other three things.

These thrusts create the framework we are working in to make progress in defense intelligence. I thought I'd show them to you as the dance-off slide and then take your questions for the rest of the time.

Student: "Asymmetric threat" has obviously become a very "popular darling" term that everyone is using of late. The problem when somebody coins a new phrase defining the threat is that eventually everybody starts finding that kind of threat under every rock, as long as they can redefine it. We had a discussion earlier with Professor Oettinger about looking at threats from a cost perspective or capacity perspective. Depending on the way you look at them, just about any two threats compared to each other can be asymmetric in some sense. How do you maintain the focus on what you're looking at, given that background? I'm wondering if a year or two from now everything will be defined as an asymmetric threat, and then the definition will lose its value in terms of what you're trying to focus on.

Wilson: The issue is not trying to find more threats. The issue is: Can you develop a system of indications and warning [I&W] that is appropriate to understanding when you are about to be attacked or have one of these threats employed against you? For example, the I&W system that was put in place for the generation of nuclear warfare force by the Soviet Union (i.e., using nuclear bombers, submarines, and ICBMs [intercontinental ballistic missiles]) is not the same I&W system that's going to warn you if a cyber attack is about to occur. The ability to understand proliferation and the indicators of state- or even nonstate-sanctioned proliferation, especially of

technologies that have dual use, does not involve the same system that works for analyzing armies and navies and air forces.

We know what the threats are. In fact, we have prioritized them. The ones that we're working on on a priority basis are exactly the ones I mentioned: terrorism, proliferation of WMD, and information warfare. What we're doing in this area is trying to bring in new analytical methodologies, new I&W methodologies, and new concepts of operations that allow us to analyze and address these threats better. Our approaches include new automated tools that are designed to help us understand the data better; data mining, so we can get through volumes of information faster; and partnering with people and organizations that have not been traditional partners, such as law enforcement, the Customs service, and border guards, to combat threats to the homeland. That's what we're trying to do, not just uncover new asymmetric threats.

Oettinger: On the partnering idea and on the difference between the threats now and the Soviet threats, let me go back to World War II for a moment, and you'll see why. A lot of lives were lost and a lot of money was spent getting weather intelligence, which was critical to convoying, to antisubmarine warfare, and to D-Day. In 2001, weather information of that caliber and then some is available to anyone with a television set, and the sources include satellites and ground observations. The globe is essentially covered with it. It has ceased to be an intelligence problem.

Wilson: As long as somebody doesn't take our weather satellites away from us. That would be an asymmetric threat.

Oettinger: But, you see, then the other guy risks blinding himself as well, so it becomes a much more complicated issue. You're essentially asking my question. When people talk about open source intelligence, they always have the image of somebody's database and so on. The weather thing intrigues me, because it seems to me that it is something that has gotten out of the realm of intelligence and into a sort of public domain where everybody's reliance on it is so high that the incentives to screw it up may diminish. Does this make any sense?

Wilson: The same could be said about GPS. Everybody, not just the military, relies on GPS. That's the kind of thing we're concerned about adversaries taking away from us.

Oettinger: But at what point are they relying on that as much as we are? It would make more sense to make them realize they are blinding themselves as much as us.

Wilson: If we're a power-projection, globally deployed force, we may need to know what the weather is in some place far from the United States. If they're there, they know what it is. It's a different hierarchy of needs if you're going to be a global power and have a global presence. I think that there are so many ways now to determine the weather that it may not be so easy to deny as some other things, but GPS is a good example.

Student: Another aspect of asymmetry would be that, if they take GPS away from us, our people aren't trained any more with the good old compass. That brings us to what we were talking about during General Moorman's presentation last week, which was that our soldiers could be calling in

and asking, "Where are we?" and our GPS is down, whereas the enemy may still have the good old compass.[5] That may be another aspect of asymmetric warfare, along with the cost.

Student: Certainly, thinking everybody's at the same low level if you're at a higher technical level is asymmetry.

Student: I'd like to hear your view of asymmetric strategies from the user's perspective. It seems to me the incentives are somewhat mixed. If you look at, for example, short-range ballistic missile attacks against Taiwan as an asymmetric strategy, it's sort of a double-edged sword. On the one hand it could be completely ineffective and, in essence, China then loses its "silver bullet." On the other hand, it might invite U.S. intervention at a much more accelerated rate, which would also defeat China's policy objective. Where do you see all this?

Wilson: I'm not sure asymmetry depends upon the view of the target, and I'm not sure what China's or Taiwan's view would be. Conventional missile attacks on Taiwan by China—not using WMD or chemical or biological weapons—would be essentially their form of artillery war, and it would be designed to have a major psychological impact on Taiwan, on a relative scale, with the long-term goal being to make Taiwan a weaker military opponent of China. It's the stronger, more capable military power inflicting the damage. The use of those same missiles, whether they carry high explosives or chemical weapons, against our bases in Okinawa or elsewhere to deny us ports of entry, staging bases, or things like that would be more what I would consider an asymmetric counter to a superior military force. It's a good example. In one case, it's a superior power using its superior military capability in a more dramatic way; in the other case, it's the same capability being used against a superior force to have an asymmetric impact.

I think that, for the Chinese, it would be a huge step to start actually striking Taiwan with conventional missiles. It would be a humongous step for them to strike another country, even if the target is a U.S. base, with WMD. There's a whole different scale of decisionmaking involved in that.

Student: Earlier on, you speculated on why attacks haven't occurred yet. I would love to hear what is on the list of why they haven't done it. For instance, why don't terrorists use biological weapons? If you look at the last five years, there are probably more deaths in the United States from high school shootings than there are from biological weapons. From a U.S. viewpoint, perhaps you should address high school shootings rather than biological weapons.

Wilson: That's more to the point for the Federal Bureau of Investigation; that's domestic intelligence. There is a classic debate why terrorists, such as Osama bin Laden, have not used chemical or biological weapons against the United States. Is it because they don't have the capability yet, or is there some deterrent to their attempt? Personally, because we don't know for sure, I tend to default to the point that something is still deterring that from occurring.

In the biological weapons arena, you can't be sure what chain of events you're really allowing to occur. If you trigger a contagious infectious disease near your own country, you may be unleashing something that you can't control. You cross thresholds. Let's say bin Laden wants

---

[5]See Thomas S. Moorman, Jr., "The Commission to Assess U.S. National Security Space Management and Organization," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2001* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-01-3, November 2001), [On-line]. URL: http://www.pirp.harvard.edu/pubs/html

the United States out of the Arabian Peninsula. If he uses a chemical or biological weapon somewhere, he could create mass casualties. Is he going to achieve the desired result, or is he going to mobilize world opinion against him in a linked way that he can't control? I don't know the answers. They're all interesting questions.

Oettinger: Are enough resources expended to address that kind of question? Remember, during the cold war there were periods when the Soviets were alleged to be plotting to poison our water supply. You get in a position where the question "why doesn't it happen?" is underaddressed.

Wilson: Our normal approach is to find out whether people really have the capability to make it happen. We know that if a country makes it happen and it is traceable, that country has to be concerned about the response. If it's a nontraceable action, it's a real capability issue: maybe people who are not traceable don't have the capability, or maybe there's something that deters them.

Whether enough resources are spent on it, I don't know. We're certainly spending more resources on trying to understand the capability and the intent of various groups. In terms of understanding how we could deter them, it's probably a very useful thing for policymakers and operators to pursue. Why didn't Iraq use chemical weapons in the Gulf War? I think some would say that they got the message that we had our own WMD, and that was a pretty clear deterrent.

Student: This is on another topic, because of the president's national missile defense speech a couple of days ago.[6] What do you think is more likely, a foreign power using a missile tipped with a weapon of mass destruction or what we were just talking about?

Wilson: You sound like Senator Levin![7] He asked me that same question in a hearing on worldwide threats. I personally think the latter is more likely: a terrorist event against the United States with WMD is more likely than a missile attack, which could most certainly be attributed to the country of origin. The real area of debate is to what degree countries with missiles can use them for blackmail and achieve their purpose because of the threat, not necessarily the execution of the threat. As the intelligence guy, I can say which is more likely, but I don't have the luxury—nor do I really want the luxury—of saying which one we have to work against. We have to work against both, with pretty much equal vigor.

Student: A few weeks ago we talked about there being a kind of growth in the intelligence community, especially in the joint military sectors. There seemed to be a proliferation now that each unified or specified command has its own intelligence organization.

Wilson: I don't know what your question is, but the premise is incorrect. But go on.

Student: I was wondering how the DIA fits into the military intelligence picture, and what your relationship is to your sister intelligence agencies.

Oettinger: May I rescue him on the first statement before you get too involved in this topic? The class read a draft statement by Jim Simon in which he didn't speak of absolute growth but the

---

[6]President George W. Bush gave his speech on national missile defense on May 1, 2001.

[7]Carl Levin, Democrat from Michigan.

rapid shift of assets and influence to the commanders in chief relative to the center.[8] I think that's what he was referring to, and I just want it to go on record.

Wilson: I wasn't being cruel there. It's just that I'm so trigger-loaded to respond to that question of growth in the intelligence community. What has grown are the requirements. In fact, it might be useful for me to give you the real skinny on that.

At the time of Desert Storm my program, the GDIP, had about 24,000 billets worldwide: in Washington, in the military services, and in the unified commands. Except for the DIA, they were mostly in the service organizations. The military filled the billets at about 95 percent. In 2001, we have about 17,000 billets in that same setup, and they are filled by the military at about 85 percent. The numbers inching down to about 16,000. That still sounds like a lot of people, but if you have a thousand watch positions in the world that operate twenty-four hours a day, seven days a week, which you are doing forever, that takes 5,000 people right there. The fact is that we have shrunk significantly since 1991, and we have gone much more joint. Even the commands have gone down a lot in total intelligence manpower, from about 5,000 people in the commands to about 3,500 today, but they have shifted from being in the military intelligence service organizations to being in joint intelligence centers at the unified commands.

When the vice president asked a question about comparing 1991 to 2001, I told him, "We're a lot smaller, we're a lot more joint, but we're also a lot better connected." We have high-bandwidth communications, classified intranets that allow us to work collaboratively, and all that kind of stuff. We are a lot better coordinated, and we have written a joint doctrine on TTP to facilitate joint operations and federated battle-damage assessment and targeting. I think we operate better as a system than we used to.

The issue about requirements is interesting. I was testifying before the Senate Armed Services Committee last year, and one of the senators asked me a question based on the same premise you used: "Admiral, it's been ten years since the end of the cold war. When are we going to get the peace dividend in intelligence?"

I said, "Senator, it's an interesting question you asked, because we are now one hour and fifteen minutes into the questions and answers, and this is the first question we've gotten that's not about Russia, our cold war adversary." For an hour and fifteen minutes, it was: "Admiral, tell me about the impact of Chechnya on Russia conventional force strength." "Is organized crime in Russia likely to cause a higher incidence of nuclear material proliferation?" "Do we believe that Russian nuclear weapons are solidly under civilian command and control?" On and on like that. I said, "We never got those questions in the cold war: 'Do they have solid command and control of their nuclear weapons?' 'Chechnya?'" Now they want to know with more precision, more depth, about Russia than they ever wanted to know before, and they want to know about a peace dividend, and we haven't even gotten to China versus Taiwan, India versus Pakistan, Korea, the Middle East, WMD, information operations, which we never talked about in the cold war. The perception is that we've gotten bigger, and we really have gotten a lot smaller.

As to the other agencies, I am the de facto DMI, and there is, I think, a very good and close coordination between the DIA, the service intelligence centers—Army, Navy, Air Force, Marine

---

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

echelon-above-corps intelligence centers,[9] which primarily gather technical intelligence in support of modernization, weapons acquisition, and threats in related areas. They do foreign materiel exploitation; they look at foreign technology, tactics, techniques, and procedures, and stuff like that. There are very regular interactions between them, the DIA, and the unified command joint intelligence centers, and we conduct collaborative analysis, all empowered by advances in connectivity and databases.

With the Central Intelligence Agency [CIA] there is a fair degree of overlap on some topics. Some will say it's duplicative; others will say it's a healthy situation to have different eyes on the target. Personally, I think that, for the most significant threats to the United States, it's worth having a little duplication to get different perspectives. We come at things from different angles, because we have different customer sets. Writing for the national decisionmakers—the president, the secretary of the treasury, and those people—is different from writing for a unified commander in chief or a joint task force commander, as we do. Actually, writing is not the issue. A lot of our stuff is not written at all. It's digitally disseminated to a command center display, or even to a weapons system in the military.

On the counterterrorism side, the DIA focuses on trying to provide strategic analysis and warning. The CIA is also focused on that, but mainly to support its own counterterrorist operations.

I think we generally coordinate fairly well. The NIEs are the product of an organization that drafts them, but the intelligence community and the National Foreign Intelligence Board, which I sit on, then hammers out each one at a table like this, in terms of the final draft, president's summary, and the key judgments. They are a collaborative effort of the intelligence community, not the products of any one agency.

Student: Following up a bit on that theme, several years ago General Clapper spoke at the seminar about being the de facto DMI and pointed out that the director of central intelligence is also the director of the CIA, and that might not in fact be the best way of organizing things.[10] Perhaps that's a sensitive topic, but I was curious about your opinion as to perhaps having one person be the DCI and another person be the director of the CIA.

Wilson: In a perfect world, I might prefer that the DCI be a separate person with a separate community staff sitting somewhere different, away from all the agencies. The current DCI is a good friend of mine; he's a wonderful American and he does great work, and I'm fully supportive of him and very happy with the way he runs things, but, divorcing it from personalities, I personally think that maybe a separate DCI who doesn't also have to run an agency would be good for the community. Right now, the new administration is examining everything, all kinds of military organizational lashups and the intelligence community. There's a "let a hundred flowers bloom" campaign on studies.

---

[9]Echelon above corps is a level above the largest fighting unit of a particular service. In this case, the centers might report to the CINC of a unified or specified command or a joint task force.

[10]James R. Clapper, Jr., "A Proposed Restructuring of the Intelligence Community," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1996* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-97-1, January 1997), [On-line]. URL: http://www.pirp.harvard.edu/pubs/html

Oettinger: What would you say to a counterargument, which is that a DCI, like a DMI, without his agency would be sort of a sitting duck out there on cloud nine, with no chips to play with.

Wilson: It depends on what you want the DCI's role to be. If the DCI's role is to manage the entire community, make sure the entire customer set is adequately and equally addressed, and serve as an advocate for military intelligence, tactical intelligence, and everything, there are lots of pros and cons. People could say exactly the same thing about the DMI and the services: would it be better if the DMI were not the director of the DIA?

Student: Going back to coordination, we talked about the situation within the United States military, but how is it with allies, especially NATO? How effective is the sharing, and how much do you share?

Wilson: We share a lot with NATO. We have a fifty-year tradition of preparing to conduct war together with NATO countries if one of them is attacked, so there is a widespread mechanism for sharing. There is an automated system for sharing, and there is a NATO procedure to coordinate and produce threat documents. Certainly anyone who has been involved in the NATO process would say that any situation where you have to get nineteen countries to agree to something, which is what is required with NATO, is a challenge. There is a process, or a system, to do that. Of course, NATO is now focused on other things than what it was focused on during the cold war, just as we are. The Kosovo campaign [1999] was the only time NATO has ever engaged in combat as an alliance, and it was not what anyone had ever envisioned. NATO wasn't built for that. NATO was a defensive alliance that was ultimately used to intervene in a European crisis, the Balkans.

Student: How many DIA resources were used by NATO? When you suddenly shifted from defensive to offensive, did you turn on the intelligence?

Wilson: We provide regular, daily infusions of intelligence to NATO headquarters and to Supreme Headquarters, Allied Powers, Europe [SHAPE]. We did that during Kosovo as well.

Student: Do you have a high-level person from the DIA at NATO headquarters in Brussels?

Wilson: Yes. Actually, the NATO director of intelligence, filling a NATO position, is a DIA employee, a civilian senior executive service person. That position has traditionally been filled by a military officer, a two-star general. Countries would nominate people. In many cases, they would nominate an infantry officer or an armored officer or an admiral who didn't have intelligence experience. A few years ago, when it came time to nominate, the United States didn't nominate a military intelligence officer but put up a career defense intelligence civilian who understands intelligence, and NATO selected him. They just selected another U.S. nominee who is a DIA civilian intelligence professional.

Student: If you're down a third now in numbers relative to a decade ago, even with I assume a force multiplier effect of the technology, what number of people do you think you need ideally, given the increased complexity of the threats you're looking at now vis-à-vis ten years ago? Also, what percentage should be civilian? Is that 60 percent a good number?

Wilson: I think it's very hard to come up with the right number. It should be requirements driven. Right now, we're barely holding our own on the traditional requirements, but being able aggressively to address things such as information warfare, information operations, biological

warfare, and the other kinds of things I've been talking about will take an additional investment in manpower to do well. We're trying to increase our counterterrorism account—not only analysts, by the way, but also collectors, case officers, people on the streets—by several hundred people to get depth and breadth of analysis.

I really haven't thought about the total number. I don't think it necessarily has to be 24,000 again. I'd be happy to get our unfilled billets filled. We have over 1,300 unfilled billets in the GDIP. That's a lot of manpower right there, but that's a reflection of the current military manning problems we have in the DOD in terms of recruiting and retention.

The DIA is 60 percent civilian, 40 percent military. The unified commands are more or less the reverse: they're more like 65 percent military, 35 percent civilian. I think it's a fairly good mix right now. The civilians in the DIA and the commands give you long-term continuity on problems. A lot of the civilian manpower is in information technology and some other support fields. They're not necessarily all analysts or collectors. Most of our civilians, or a good portion of them, have military experience. They were in the military for a while; in fact, a lot of them are people who retired from the military after twenty years and then continued in intelligence. I think the ratio is pretty good. I would not like to go too much lower on military manpower than we are. It's certainly critical for our program to have the military coming back into the DIA after being afloat, or in a division, or in a brigade doing intelligence at the operational level.

Student: Could you just expand a little on the question of requirements going up and the numbers of people going down? Could you say a bit about having the intelligence reserve component engaged more than they were a few years ago and how that has helped or not helped, or is it still a work in progress?

Wilson: The reserve component has been a tremendous help. About fifteen or seventeen years ago, Secretary of the Navy John Lehman said there are three things in the Navy reserves. One is Maritime Patrol Aviation, the Reserve P-3 squadrons that hunt for submarines. The second is the reserve Naval Construction Brigade—they go out on the weekends and they build stuff, and it doesn't matter if they go on Saturday or Sunday. The third is intelligence—they are producing and writing intelligence about long-term issues on the weekends, and that becomes an important percentage of our production.

I would say that the use of the reserves in intelligence has really gone up and become more important, and they have been tremendously empowered by the information revolution. We have twenty-seven Joint Reserve Intelligence Centers around the country, at Army–Navy–Air Force–Marine bases, where people drill jointly and where we put "full-time augmentee" in as an active duty. The fact that they can be connected and working on a classified intranet, a collaborative environment, just as though they were sitting in the next office at the DIA or the Naval Intelligence Command, Office of Naval Intelligence, is a tremendous enabler for the reserves. They are only increasing in importance and doing tremendous work for us every day. With a whole lot of guys recalled to active duty for operations in the Balkans and elsewhere, we would be in bad shape without the reserve component, for sure.

Student: Admiral, could you talk about the revitalization of the work force? How is the DIA recruiting new "meat" to take care of all the old people who are retiring?

Wilson: Right now, our attrition is not too bad, but here's an interesting thing about the DIA. We talk about "restructuring for a new world order." We have a great variety of threats out there, and all sorts of new intelligence topics, and the situation requires great agility and flexibility. The same is true in the human resources world.

The DIA wanted to hire 300 people in FY2000. That was our goal, because that was our projected attrition. We were only able to hire about 231, and we had 10,000 resumes on file. You say to yourself, "Why the hell is that? Is it that you can't find 300 qualified people out of 10,000?" The answer is that you not only have a cold war bureaucracy in intelligence, but you also have layers of bureaucracy in human resources. We had trouble processing all this stuff. The system didn't allow it. You're at a college campus, and you're talking with someone who has a 3.8 grade point average, a dual major in international relations and biotechnology, speaks two languages, is captain of the volleyball team, is in the concert band, and has a spotless record. You say, "I can get you an interview, and we'll get back to you in eight or ten months." You should be able to say, "Oh, really? Would you like to sign up right now as a conditional hire? I think we can find a place for you in our workforce."

This year we need about 400 people. We're only about halfway through the fiscal year, and we've already either hired or made offers to hire almost 300. We put in an automated resume processing review. We have a corporate hiring board now where we can screen the resumes and make decisions to hire people a lot faster. We were actually given authority to make on-the-spot conditional hiring offers. Together with the rest of the intelligence community we are developing a corporate, community recruiting Web site. You can go into that site and learn about the intelligence community and get hyperlinked to each of the agencies.

One of the big things is that we've cut down on our security investigation time from whatever it was to about thirty days for uncomplicated cases. You have to be eligible for access to sensitive compartmented information. The military is taking nine or ten months right now; there's a 500,000-case backlog with the Defense Security Service. We're doing contract investigations and our own adjudication. We can usually get uncomplicated cases—people who haven't done a lot of overseas travel and things like that—on board and cleared about thirty days after we receive their completed paperwork. Even complicated cases we can get on board in about forty-five days, if they're willing to take a counterespionage-scope polygraph. We are trying to do a whole lot of things in terms of flexibility and agility so that we can replenish the workforce, because there's a big bulge of people who are reaching retirement age in the next five or six years and this problem will get even more demanding.

We're also not automatically replacing billets without review. If the person who is retiring is a certain kind of analyst, do we need to hire that kind of analyst or should we hire an information technologist? We're trying to review every billet and see what kinds of skill sets we need in the future. We have a whole lot of other human resources things going on, and kind of a human resources campaign in the DIA. I could go on about that too, but I don't want to wear you out.

Oettinger: Something you said a little bit earlier led me to believe—and you can correct me if I'm wrong—that you, the DIA, are still sort of thinking in terms of lifelong careers. Mike Hayden gave us a pitch where he figured that at the National Security Agency [NSA] the recruiting pitch

would be more like: "This is a great starting job, but not necessarily one where you would spend your life."[11] Is there a difference in aim, or clientele, or am I just mishearing?

Wilson: Actually, I've had this discussion with our Gen-Xers. Everybody says, "The new people who come into the work force want to have the ability to move quickly and move here and there, get out of government and back into government." We have about 600 or 700 entry-level people who came in since 1996, and I've had meetings with them. I asked them directly: "Should I build a program that makes it easy for you to leave and come back and appeal to that sense of mobility and flexibility, or should we concentrate on building an environment that makes you want to stay for thirty-five years in this organization because you like the work and you like the work environment?" By far the majority said, "You ought to try to build an organization where people want to stay in." So my instincts are that we should try to be more flexible, and be able to accommodate people leaving and coming back more easily than we have in the past, but should concentrate on the longer term.

I think that we have an extraordinarily appealing mission. Security work that defends the nation is motivating, it's interesting, and there's a lot of opportunity for diversity in the jobs within the DIA and the intelligence community. We have programs to move people within the community and then come back. We have programs to put them out in the unified commands overseas and in the defense human intelligence [HUMINT] service. There are all kinds of opportunities. I think we should try to build an environment that actually makes people want to stay for a long time because they like it and they feel gratified by the work. I would tend to disagree a little bit with Mike. I think you have to accommodate that aspect of the workforce, but you might want to shoot for higher and loftier goals. I'd be interested in your opinions, by the way.

Student: Do you have programs so people can move among the DIA, the CIA, and the NSA?

Wilson: There is an intelligence community rotation program. In fact, you can't be promoted to the senior executive service unless you have done at least one tour outside your agency in one of the other intelligence agencies—the services or the CIA—so we certainly have a program of rotational assignments and augmentations and things like that.

Student: As a Gen-Xer with intelligence community experience, I think probably the biggest issue for us is the ability to be promoted on the basis of merit, rather than time in grade. I know that a lot of people who are my age are frustrated with these bulges that you get. A lot of times you can't move up to a GS-13 or GS-14 position until someone from that position leaves the company or moves up another step. So I was wondering, is the DIA doing things to help with retention as far as this is concerned?

Wilson: It's a tough issue, because the real issue is managing personnel cost and the unconstrained growth of that cost. At the rate we're going, in 2007 our personnel cost will be 58 percent of our budget, and that's an untenable situation. It's not just salaries, but medical benefits and retirement. The workforce that we have in the GDIP, which is 7,000 smaller than it was in FY1991, costs a lot more. Finding ways to manage that personnel cost growth and facilitate

[11]See Michael V. Hayden, "The Roles and Responsibilities of the National Security Agency" [working title], in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2001* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-01-3, 2001), [forthcoming].

promotions and rewards is a very demanding challenge unless we have some increase in top-line resources.

We also have a bad inverse pyramid. We've got too many GS-14s and GS-15s in the DIA, 33 percent of our work force, because you have to promote people to give them the salaries they deserve, and in general promoting people in the government means they have to get more into management or leadership positions. Sometimes you want to promote people or give them more money just because they're good technicians or good analysts or good case officers.

In the human resources business, we're trying to examine ways to accommodate all of those concerns we sometimes have about retention. For example, do we always have to promote people and give them more managerial responsibility, or, based on their accomplishments, can we give higher cash awards and bonuses? I'm actually cutting back the number of people who get cash awards and bonuses in the DIA. A big shock for our defense intelligence senior-level people in the last month was that, whereas before 80 percent of people got cash awards and bonuses, this year it's less than 50 percent, but those who got them got bigger ones. I'm in favor of giving bigger cash awards and bonuses to fewer people, the ones who really deserve them, as opposed to its becoming an expectation that you get a salary augment at the end of the year.

I'm also in favor, by the way, of giving cash awards and bonuses to people who produce well as a team. I'd like to reward a team of analysts who do extraordinarily good projects for what their team produced as opposed to rewarding the guy who briefed the results. We're trying to accommodate all these concerns.

We've also been competing with a very strong job market in the last couple of years. The competition is not quite as tough right now. I don't want to make you feel bad, but a lot of information technology people are trying to come back into government right now.

Oettinger: There was a story in the *Wall Street Journal* yesterday about a once-upon-a-time millionaire now applying to the Harvard Business School.

Student: At the risk of rehashing an earlier conversation, the bonuses only work for the 60 percent who are civilians. If you changed the ratio and made it a higher percentage of military versus civilian, would it help that problem or just turn it into a different kind of problem?

Wilson: Right now, it's not an option, because the military can't fill the billets we have. It's not a strategy that's attractive to me. I think the ratios are about right, for a lot of reasons. To answer your question, I think our enlisted population of noncommissioned officers [NCOs] is enormously capable and is sometimes underutilized. The cost of enlisted billets is a lot less than officer billets. There are a lot of areas where we could probably use more enlisted manpower, but that is hard to come by, too, because the services are (rightly, in my view) putting priority on manning wings and brigades and ships, which are at the pointy end of the spear. I think right now there's no logical way to try to control costs by using more military. In fact, right now the military billets are the most expensive ones I have. You know why? Because I'm paying for over 1,300 of them that are not filled. That makes the average cost of the filled billet pretty high.

Student: Admiral, could you talk a little bit about the attaché corps? Is it expanding or increasing the missions, and in which geographic areas?

Wilson: We have over 900 people in the attaché system right now. There are attaché offices in more than 120 countries, and representation in about 175 countries. A few places where they're

based cover multiple countries from one office. We're trying to expand it. We want to put more open attaché offices in more embassies, mostly in Africa and South America, where we had pulled back in the mid-1990s, and we're trying to beef up attaché presence in some other countries. It's a little difficult to expand because we have one congressional committee that's not too keen on it, even though the other five like the idea.

The attaché system is well supported right now. For the Army, we just received the promotion results to colonel. I think in our defense HUMINT service directorate of operations there was about a 70 percent selection rate, which was above the Army average, and among the attachés it was 100 percent. So that's a good signal from the Army.

The attachés are doing great work in a number of areas. They are great jobs, and wonderful opportunities for families to go overseas and work together (the spouse and the attaché) in the military–diplomatic–intelligence arena.

Student: Are a lot of our attachés being recalled from Moscow as a result of national politics?

Wilson: They're not being recalled; we had three booted. They haven't actually left. They were not PNG—*persona non grata*—but it was pure retaliation, because we expelled fifty Russians (or we expelled six, and forty-six more are to leave by July 1, including their army, navy, and air force attachés). Ours were in the same positions. It was a symmetrical response. The big issue now is the battle over visas for the new attachés.

Student: What is the JMIC doing these days?

Wilson: The JMIC has about 450 students. One-third of them are full time, and the other two-thirds are going on weekends and nights, because we operate seven days a week. We're giving about 150 master of science [M.S.] degrees in strategic intelligence a year. Almost everybody who goes through the program thinks it's a very good, academically rigorous program. The master's theses may be classified or unclassified. We also have a bachelor of science in strategic intelligence, where we give the fourth year for people who have gotten three years of college on their own. It's a wonderful tool to give a degree to an NCO or to a secretary. We use it for upward mobility programs, to transition people from support assistance into the intelligence work force.

I have to tell you a story: I spoke at the JMIC a couple of weeks ago, and then I went down to the cafeteria and had lunch with a Navy first-class petty officer, an E-6. He was a motor machinist mate first class, which means he basically fixes engines on small boats and craft. He was a SEAL [member of a Navy Sea-Air-Land unit], so he was also a combat motor machinist mate, and he was a great sailor. Two years ago he had finished three years of college on his own, as an enlisted man, and was trying to get his fourth year, so the Navy sent him to the JMIC to get a bachelor of science in strategic intelligence. Now they're trying to get him placed into the right SEAL team next shot, so they kept him around for another year, and he gets his master's at the end of this summer. He may be the only guy in the nation who has both an M.S. in strategic intelligence and can also fix a small engine.

Student: Holding his breath under water!

Wilson: I'm hoping he goes to Officer Candidate School, or that we can recruit him for the DIA or the defense HUMINT service.

Student: Would he qualify for you on the spot?

Wilson: I do not target our military as potential civilian employees. We could certainly get him into the workforce as a petty officer. Any more questions, or do I get the hook?

Oettinger: Regretfully, the latter. I thank you, and here is a small token of our large appreciation.

Wilson: Thank you very much.

Acronyms

CIA	Central Intelligence Agency
CND	computer network defense
COP	common operational picture
DCI	director of central intelligence
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DMI	director of military intelligence
DOD	Department of Defense
GDIP	General Defense Intelligence Program
GPS	Global Positioning System
HUMINT	human intelligence
I&W	indications and warning
JMIC	Joint Military Intelligence College
JTF	joint task force
M.S.	master of science
NATO	North Atlantic Treaty Organization
NCO	noncommissioned officer
NIE	National Intelligence Estimate
NSA	National Security Agency
SEAL	member of a U.S. Navy Sea-Air-Land unit
TTP	tactics, techniques, and procedures
WMD	weapons of mass destruction

INCSEMINAR2001

ISBN 1-879716-76-3