

This panel was congressionally commissioned in 2001. We operated from 2002 to 2004, provided a summary report which is available to you on the Internet, from the government, unclassified. And, we were reconstituted by the Congress and operated from 2004 to-- excuse me, 2006 to 2008, and produced a bunch of products, but unclassified report on civil infrastructure protection. Some of our products were classified, as you might imagine.

The charter of the commission was to assess the threat, assess the magnitude of its consequences. What was our capability to protect, recover and repair, and to recommend steps for things to do about the subject. I'm going to put the commissioners up here because, if you read my bio, you would not know that I was an EMP expert. And the only reason I claim any expertise now is that I listened to this group for four years.

But, on here, the group was led by Bill Graham who, in addition to being science advisor to President Reagan, was also a long history in nuclear effects. We have, here, weapons designers, weapons effects experts, and technology leaders and command leaders. So, the credibility of the report and the information is mercifully broader than my background.

Let me say about him. Trying to explain what is EMP, why we're vulnerable, and what to do about it in 15 minutes is a challenge. But, here is the first round. If you take a nuclear weapon and you detonate it above the atmosphere, it will release a bunch of gamma rays. And, the gamma rays rain down over a very broad area. And, they meet a thinly populated atmosphere. And, they knock electrons off the molecules in the atmosphere.

And, these highly energized electrons find it necessary to follow the magnetic lines of the earth that are in the way, that are in the region. And, this happens in [noise] in a sequential way. And, it produces a very large antenna, which radiates very high electric fields on the surface of the earth. And, that's the early time mechanism, E-1.

It is similar to lightning, in many respects, in terms of that the manifestation is kilovolts-per-meter. I've got a chart here that shows what the spectrum or the time domain of lightning looks like. And then, you will notice that the EMP has a much faster rise time and, thus, a much broader spectrum. And, therefore, it contends with lightning protection in a different way. And, you cannot count on lightning protection.

The other difference is that lightning tends to be localized and EMP is simultaneous, very high-level, and broadly distributed simultaneously. And so, there is a difference in terms of what EMP phenomena looks like.

There is another phenomenon that, having affected an ionized region in magnetic field, and radiated-- created a lot of heat in the process, the heat distorts the ionized atmosphere and also distorts the magnetic field, which causes a counter-effect on the earth. And thus, you get ground currents and a magnetic coupling to things on the earth, particularly long wires such as in the power grid system. And, this is called the E-3 effect. This is not an electromagnetic voltage effect. This is a magnetic effect. And, it is coupled to the earth to several kinds of infrastructure.

I put geomagnetic storms in here to make the point that the magnetically coupled E-3 is very similar to the effect that would occur from a solar storm that rains ionized particles on the earth, gets it channeled into the magnetic field, shows up as Aurora Borealis in a harmless way, but also affects power grids, particularly in the northern latitudes.

In 1989, there was a big outage in Quebec. The United Kingdom, for example, because of their latitude, as well as the Scandinavian countries, are very sensitive to this and have EMP warning philosophy, and so forth. But I put it on here to show that there are natural effects that also threaten us, that are similar to the E-3 of an EMP effect.

Now, it's very hard to capture this-- one of these in captivity, because you need a nuclear detonation high above the altitude in a thin atmosphere, in order to produce the

effect. So, there are folks who say, "I wonder if it really exists because we've never seen one exactly in nature." We did see this in nature. But it was also a little bit of a surprise to some people because we hadn't anticipated it.

The first picture I have on the left to you, up there, is a couple of pictures from Starfish Prime, which was a nuclear test in 1962, which knocked out things in Hawaii and demonstrated other effects for which we had not adequately instrumented the test. Let me move on.

The Russians, of course, knew about all this the same as we did. And, they actually ran tests. They are a little more aggressive in their testing. But, they proved to themselves that this was a real effect. And, both sides, during the Cold War, presumed this effect to be true, understood the physics that caused it to be true, created weapons they had the reason to believe that each side created the weapons to create EMP.

Both sides calculated that these kinds of weapons would be early used in any RISOP-SIOP exchange or nuclear exchange, with low warning time, probably from submarines offshore, in each case, which would give you less warning time. And thus, this EMP effect might neutralize, thin down the weapons that you might have launched out from under and, certainly, the commanding control systems that you had. There was some asymmetry between us and the Soviets. But, nonetheless, we both thought of it in the same way. And, we both believed that that was the case. And our systems today, many of our systems still imagine that such a threat is around.

This is just a geometry lesson. But, it's also philosophically. The commission decided that EMP, after our study, is one of the small number of threats that may be an existential threat to the nation. It may hold-- It may actually, if we do not do enough about it, be able to cause such devastation to our civil infrastructure and, potentially, our nuclear strategic capability, that we would-- we would, if that scenario applied, we would find ourselves in very serious catastrophic difficulty. And, if they were not used, they

would be used as we dealt in the Cold War with a potentially serious military threat to us.

So, it's not the only threat. There are-- Cyber is clearly a threat. There are just straight physical threats. But, this is a threat. And, if we know that it is a threat, and if we do nothing about it, there is a serious risk that we are going to invite attack by someone. We knew, in the Soviet case, what the-- that we were going to have to contend with it. But, we did not deal with the civil infrastructure as much because, in all the scenarios we thought about, it is true the civil infrastructure would have been wiped out. But, it was going to be wiped out pretty soon anyhow by a rain of destructive kinetic activity.

There is a couple view graphs here just to indicate that we had an approach. We sponsored research. We looked at, not only the military, but also the civil infrastructure, including, depending on how you calculated it, some special studies on satellites, the outcome of which were mostly classified.

And, I think-- Let me just move onto the next view graph if I can do this. I've gone through that we're accustomed to this in the military force, and particularly in the strategic force arena, where weapons such as the ICBM force and ballistic missile programs and the airborne leg of the triad made serious attempts, and mostly successful, at providing EMP defensive capability, particularly for the weapon and probably for the command and control at its best.

So, we're accustomed to this. I would say that the end of the Cold War relaxed the discipline, so that there are elements of the strategic force warning command and control and delivery systems that you would want to examine really closely if you were really serious about this, because the discipline is not as much as it was. It doesn't mean that the people aren't trying. It's just, I would say, from our examination, the discipline is not as intense. For example, when we looked at the long upcoming tanker program, it was not clear to us that the tankers were going to be EMP hardened, as an example.

The general purpose forces, there is a military requirement or specification for how to deal with EMP threats. There's a level to which the threat should be taken seriously. And, the Army, in particular, has done a fairly good job at making its weapons, its units capable of being EMP protected when buttoned up.

However, the specification is a procurement spec. It's for the hardware. It is not a systems spec in the field that systems so very often are hardened. Capabilities go into the field with a soft network structure surrounding them and without adequate warning and so forth. So, there is an issue on the general purpose forces that still needs to be worried about.

The only thing I would say here is that we looked at the proliferation of commercial off the shelf. And, I would say it's something to worry about. But, it's not so clear that it made the situation any worse or any better. It's just that it requires dedication to standards, and it requires systems engineering of a systems kind to actually cause, create EMP protected forces.

My highlight of this whole report was that we are catastrophically vulnerable in the civil infrastructure business in the United States. And, the principle vulnerability is the electrical power grid. And, the United States' consists of three big power grid areas. There's the Eastern United States, the Western United States, and Texas. I don't know that there's any political significance to that. But, nonetheless, that's where it is.

And so, from not only Maine, but into Canada, down to Florida, and to the Mississippi, there is a collection of stuff. Several hundred companies are tied together to generate power, to transmit power, and to distribute power. It's one big synchronous machine. And, in July-- August of 2003, I would say a branch fell in Ohio and turned power off in Connecticut, where I live, as well as in a good share of the Northeast. And so, it is highly-- It is fragile in its makeup. And, it is sloshing about a lot of power. So, it has the

seeds of its own destruction in its nature. And, it is fragile by its size and interconnectivity. So, I'm only going to say that that's a problem.

Now, we looked at telecommunications. We looked at gas. We looked at food. We looked at air traffic control, etcetera. Generally speaking, the only true catastrophic vulnerability, in my judgment, is the electrical power grid, because that goes down, and down in large quantities, then it's down for a long time because of the parts and recovery. And, that means that almost everything else goes down as well, including the supermarkets and water and gas and so forth. So, we need to do something about the power business.

In addition, part of the power is operated by supervisory controls and data acquisition devices that permit, in this modern age, remote control of infrastructure, things like the power, like the water, like the gas, like the-- etcetera, etcetera. So, these are vulnerable to the first E-1 that is a high electronic-- the electronic voltage. And, they exist in lots of parts of the infrastructure. And I highlighted here, as one of the things one needs to fix.

This slide is used basically to demonstrate that we are highly interdependent. You can't actually have a-- You can't actually recover from power without communications. We can't have communications without the power. And so, there is an interdependence here that is a problem.

Since I'm running out of time, let me just say that there is something-- there are things that we can do. We can do quite a bit to prevent attacks. We can prepare. We can do some protection to keep it from being catastrophic. And, we can prepare to recover. And, all of this will serve as a form of deterrence. This restates that. And, let me see what else I have that I need to tell you.

The DOD is well structured to deal with its problems. The DOD is not well structured to deal with the civil infrastructure. The civil infrastructure, the DHS is accountable and

AUDIENCE: Hi, Wing Commander Andy Challen from the British Embassy for General Kehler and also Mr. Thomas. We know that the east and the Chinese and the Asians have got a very patient attitude and we've heard about the long-term reconnaissance that they take part in, and we know that the feudal system hands down the history through the generations. In the west, we are dealt a blow to that by the political agendas and the timings of how we do things. And we've heard today with the speed of reaction of space and cyberspace, how do we mitigate those factors?

DR. PFALTZGRAFF: Okay, who would like to go next? Over here, we have a question?

AUDIENCE: Brian Green with Systems Planning and Analysis, a question for General Kehler. General Schwartz talked about the need to make space systems more responsive, and I wondered if you could give us your current thinking on how to make those systems more responsive, and for whom you would make those more responsive?

DR. PFALTZGRAFF: Okay, thank you. One or two more, we have time? Please, over here?

AUDIENCE: Mr. Hermann, could you tell us what size warhead the commission looked at? The traditional view has been that only megaton class warheads can create the kind of EMP field that would be catastrophic for the U.S. economy. So could you look at that? And for Bob Joseph, what are the lasting contributions of the Bush Administration to counterproliferation, particularly the PSI?

DR. PFALTZGRAFF: Okay, one or two more? Who else would like to go? Is there one more question? Yes?

AUDIENCE: Ted McFarland from Booz Allen. This is for General Kehler. I'd like to hear your views on how industry can help with this-- you talked about cyber acquisition and the need for speed and how we can help close that gap.

DR. PFALTZGRAFF: Okay, well then let's take those questions. By the way, even though they're directed at a particular member of the panel, or members, others I hope will feel free to help to respond. So let's begin, and maybe General Kehler, since you had so many questions directed to you?

GENERAL KEHLER: Yeah, I hope these are panel responses as well. It's been so long I talked, I forgot what I said.

DR. PFALTZGRAFF: The audience hasn't forgotten what you said. [laughter]

GENERAL KEHLER: Okay, let me start with cyber, General Shaud, and your question about whole of government. No question about this, this is a whole of government issue. I think you all hear that. You certainly look at that in the articles that are being written and the discussions that are being held. Here's what we have focused on to date. The Air Force has come through a very interesting set of discussions about where we wanted to go regarding cyberspace. We made some decisions, the Chief and Secretary made some decisions a year ago at Corona about assigning lead command responsibility to Air Force Space Command, standing up 24th Air Force, going to the AF ISR Agency and having them establish a group that's going to be in direct support of 24th Air Force, giving Dick Weber, the commander of 24th Air Force command authority over the entire Air Force network, et cetera.

If you listen to all of this, this is really about getting the Air Force's house in order regarding cyberspace and starting there. I think we have done that. And here's what we've recognized in the fairly brief time that we have now been consolidating these cyber activities in this command as lead command. What we understand is that there are many lanes regarding cyberspace and that we are in one of them. We recognize

that we are not alone, really, even in the lane that we are in. Our Service colleagues are in there with us. We recognize that we are part of a Department of Defense activity that is still emerging and shaping. And we recognize, I believe, as I listen very carefully to the combatant commanders, both General Kevin Chilton, who you'll hear from at a later point in the conversation who has responsibility, unified command plan responsibility for these activities today. And as they are working their way through what the Secretary of Defense has directed us to do as a department and standing up U.S. Cyber Command, we recognize that this is a much bigger issue than the Department of Defense.

And so at this point, our focus is really, sir, on making sure that we are looking at ourselves with two major pieces; actually, three. One is doing a better job in installing the wherewithal to protect ourselves and make sure that we can assure the missions. The second is to make sure that we are able to respond to what the joint war fighters are going to need in terms of Air Force participation and how we will present forces, how we will establish those command relations and all of those mechanical things that are necessary for us to take Air Force capability to the joint team.

And then finally, what we do regarding people and how we prepare ourselves to compete, if you will, for the talent. And you heard the chief mention something about that earlier today. That will be a very interesting piece of how we will go forward. And so we are looking at some alternatives, actually, to take back to the Chief and Secretary on how we will do better on that part in terms of organizing ourselves and training and preparing our people.

We do know this is a bigger picture than us, we can tell you. And Dick Weber, who was here, could tell you that our initial activities, we are in fact supporting STRATCOM today with their activities. As I say, General Chilton is responsible for these activities today within the department. And so we know from their experiences and our component experiences with them that this is clearly a whole of government activity. In some cases, my football field analogy suggests to me that we will not be the major player in cyber and that gets back to it depends on what happens on the football field. You know, if

somebody comes in and spray paints something over a player's helmet, that's not an Air Force problem. It's somebody else's problem. If somebody hits somebody and there are civilians who happen to be passing by, that's not the football referee's problem. So this is going to be a very interesting set of authorities, responsibilities, and recognizing that we must be very mindful of protecting Constitutional rights.

DR. PFALTZGRAFF: Let's go across the panel and continue with Bob. Would you like to respond to some questions?

DR. JOSEPH: I wouldn't want to try to respond to any of the technical questions. My background in physics is just two courses deep, physics 101 and physics 101. [laughter] So let me just comment on PSI, on the proliferation security initiative. This was one of the principle tools, new tools, that the Bush Administration did put in place relatively early, I think it was May 2003. And it's one of a number of tools. The others were the globalization of cooperative threat reduction, Nunn-Lugar type programs through g8 funding, United Nations Security Council 1540, which this administration has also pushed forward.

The global initiative to combat nuclear terrorism, which is an initiative that President Bush and President Putin sponsored together, as they did with yet another initiative on managing the growth of nuclear energy in a way that hopefully will be more proliferation resistant. But these tools, and other tools like them, including in the defense area, such as missile defense, and new concepts for deterrence, have to be seen I think in the broader strategic context. And specifically in the three tier strategy that the Bush Administration put forward. And as far as I can tell, is still being implemented, at least in part by the Obama Administration.

PSI specifically has now grown to 95 countries. As most of you know, it's aimed at stopping the trade in proliferation. It has created, I believe, a more proactive sort of stance for the international community to deal with the disruption of the trade in proliferation. And it has had a number of key successes, many of them are classified

given the nature of the work that has been done through various intelligence channels. But one that does stand out is the interdiction of the BBC China in October of 2003, which did lead to the unraveling of the A. Q. Khan network as well as to the Libyan decision to abandon its nuclear, chemical and long-range missile programs.

DR. PFALTZGRAFF: Thanks, Bob. General Kehler has a comment or two more to make on questions. So let's go back to general Kehler.

GENERAL KEHLER: I didn't want to ignore the other two questions that came my way. So before we go down the rest of the panel, the question that was asked about the Chinese and sort of how we view them; just let me offer one thought about this. Remember, those of us who have children, remember when you would take the kids to the doctor for their shots when they were little? The doctor always had a blue bear. They would hold up the blue bear like this, and the kid would look and then you'd get the shot? I'm not so sure that the direct ascent ASAT isn't the blue bear. I think we need to be mindful of what the other panelists have said here about philosophy and strategic patience and strategic intent and the other things that go with that.

And so what we need to be careful of, it doesn't matter who we're talking about here, is we need to make sure, I think, that strategically we do not find ourselves in some kind of strategy that imposes things on us, that imposes costs, that imposes those kinds of difficulties on us without being certain or at least fairly certain, that we are on the right strategic path. Which gets to my point about mission assurance here. This isn't about trying to launch the equivalent of the *U.S.S. New Jersey* to orbit, which would take a lot of lift, by the way. I'd use Dr. Joseph's two physics 101 classes and tell you that that's a lot of lift that would be required.

And the second thing, someone asked about responsiveness and how we're thinking about space and space responsiveness. I believe that a responsive space capability that as strategic command has outlined to us, has tiers associated with it-- not t-e-a-r-s, t-i-e-r-s-- tiers that would start with the things that we already have and making those

more operationally responsive and goes through a series of steps that allows us to have a national strategic capability to augment or replenish or reconstitute some amount of our capability in concert with a mission assurance approach, which means that we would be looking also at air and cyber for part of that, or maybe a significant part, of that reconstitution depending on the scenario we find ourselves in.

I believe that kind of a responsive space contribution would contribute to deterrence. And that's what our objective ought to be as we go down that road. And I believe today, we have a number of elements that would need to come together to have that. We need to have responsive launch vehicles, we need to have a common command and control system so that we don't redo a command and control every time we put up a small, cheap satellite. We need to have common buses, et cetera, with standards. There are some great things going on, and I know Curt Bedke, (Major General, Commander of Air Force Research Labs) is here, the Air Force Research Lab, and elsewhere, about plug-and-play kinds of things. And then what we need are militarily useful sensors that could plug into them. So those pieces are in work at varying levels. I would tell you, I think we've got three of those four, pretty substantially in work today. We don't like what it costs, but I think in terms of a crawl/walk/run approach for national security and a strategic capability for us to contribute to deterrence, I think a responsive space capability is necessary.

DR. PFALTZGRAFF: Thank you. Bob?

DR. JOSEPH: Let me just follow up on the China ASAT. It happened, I believe it was early January of 2007, it happened on a Friday during the weekend. The State Department undertook a number of steps to coordinate the response with allies. On Monday, we called in the Chinese ambassador. I had the opportunity to do that. The Chinese ambassador sat there and responded, A, that he didn't know anything about an anti-satellite test; and B, Chinese opposed U.S. weaponization in space. Needless to say, I did have some fun in that meeting in responding.

But what we did afterwards, I think, was even more instructive. And that is we made the rounds to Congress, to argue that this is a major wakeup call and we need to change the way we approach space and particularly our vulnerabilities in space. As far as I can tell, no one's answered that wakeup call. I hope I'm wrong, but I don't believe I am.

DR. PFALTZGRAFF: Thank you. Dr. Hermann, would you like to talk about the megatonnage issue?

DR. HERMANN: Megatons, right. I can assure you that the commission spent a lot of time on that subject, and there's a couple of elements of what is technically required. And the discussion and the material and the information in those sessions were classified. And so, I can't quite, but let me say as a layman what I think I can tell you.

That both we and the Russians know how to design bombs that will create high electric fields, E&P fields with other than megatons total output. They will create the electric component. It probably takes a big bomb to create a truly disastrous magnetic E3 component.

The next question is, well, would any minor player with a handful of weapons or one or something, would they be able to have it? And then there is a contest between the intelligence community which says we see no evidence. And then there's Rumsfeld who says the absence of evidence is not the evidence of absence. And so there's a discussion as to whether somebody would have the ability to create it. But on the other hand, stealing apparently is a behavior of humans. And so stealing ones that are already developed by somebody seemed to be a possibility. So there is a question about whether or not the cheap shot by a minor player will be fulfilled by some other than a-- it won't be confined to a super power issue. And I would say I came away persuaded that I don't know what people have, but I see a plausible way for somebody to destroy my country unless we actually take modest measures to keep it from being a catastrophe.

DR. PFALTZGRAFF: Timothy Thomas?

MR. THOMAS: With regard to the question about China, I would say they already have a whole of government approach. They really do look at this whole issue holistically. There's an old saying, quantity has a quality all its own. And when you've got about 350 million Chinese who speak English, you have lots of people that they mobilize for cyberspace issues. They also have information industrial exercises over there, they have mobilization exercises quite often. So they really are practicing now in peacetime for something which doesn't sound all that good, to be quite honest with you.

Terminology seems to be to me the one bugaboo that we have in this country. We are so focused on our sound bites and we live by our sound bites and we expect others to live by our sound bites. And I think that's just one of the biggest mistakes we make. For example, take the term asymmetric warfare, I challenge anybody in this room to come up with a Chinese definition of it. They don't think like we do. Asymmetric warfare, one of the definitions I saw was the application of abnormal logic through the exercise of 12 crafty tactics. Now, that's something that we don't even come up with in this country. And if you don't understand where they're coming from, what strategy is, how they look at these terms, you really are off base from the beginning.

General Schwartz's comment this morning about we need space control, really is something that strikes at the heart of China. They look at control as more important than dominance. They would refer to something like Kosovo and say, "You had information dominance, but you still didn't have information control because the Serbs were able to influence you by some of the things they did on the ground and cause you to shoot weapons at mock-ups and those sort of things." Control is a huge issue for them and it lies at the heart of what they're doing, I think, in many different arenas.

The last thing I'd like to say is just the fact that with the football analogy, I like it. I like this whole idea of being on the playing field. The only thing I worry about is are we scouting the other team? Do we really know what the other team's doing? And if these

rules and regulations are not the same, are they playing rugby when we play soccer? Or as General Kehler said, are they the ones who are going to spray paint your face because that's part of their rules and regulations? You really have to think hard about these analogies because it isn't the same team. And if we don't scout them, if we don't know what kind of offense and defense we're playing and we know what we're doing, so what? We got to know what they're doing, too. So, thank you.

DR. PFALTZGRAFF: Dick, you have the last word?

DR. SCHULTZ: Well, I would note that the concept, whole of government, really grows out of the wars that we've actually been fighting since 2001, not ones that we might have to contemplate in the future. And that concept deals with the kind of security environment that I outlined. In Iraq, in Afghanistan and elsewhere, what we found is that we needed a different approach to conflict and security. We learned it the hard way in Iraq, but we learned it.

Now, what that means is that military forces and an array of other capabilities, or military forces doing things that other agencies of the government ought to be doing, have to come to play in order to stabilize the situation and deal with the kinds of conditions that we've been dealing with in the wars we've been fighting. How well are we doing in terms of developing this whole of government approach really is the second part of this project that I mentioned to you.

We're doing okay. To use a football analogy, since it seems prevalent here today and since I played that game for seven years, we've advanced the ball a bit, but we have a long way to go in terms of dealing with the irregular warfare. Now, remember the QDR in 2006 said this regular warfare environment was increasingly what we were going to be involved in. Secretary Gates last year said it's as important, irregular warfare, as the other kinds of warfare we may contemplate fighting in the future. But in terms of a whole of government approach, we're not there yet.

DR. PFALTZGRAFF: I would like on our collective behalf to thank this outstanding panel for its outstanding contribution in helping us to set the stage for what is to follow in this conference. I realized that we are running a few minutes behind schedule, so therefore I hope that you will make the break very brief. Certainly at the maximum, 15 minutes. We will run, of course, a little bit into the lunch hour with the next panel, which promises to be another outstanding contribution to this conference. So again, we adjourn the panel at this time and welcome the new panel in a few minutes.

END OF SESSION I