An Interview with

James E. "Hoss" Cartwright

DOD

General James E. Cartwright, USMC, is Commander, U.S. Strategic Command.

JFQ: *How do you rate the ability of U.S. Strategic Command* [USSTRATCOM] *to carry out the mission of combating WMD* [weapons of mass destruction], *and does the command have all of the authorities and policy guidance essential to this mission?*

General Cartwright: Combating WMD was the last mission area given to the command in sequence, and so from the standpoint of time to mature, it's had the least. This is a mission area that in the last Presidential election was the only area that both candidates agreed on, and they both agreed that it was the most important thing—a heretofore unassigned mission area. That gives you a sense of the importance that the National Command Authority puts on the mission, but over time it has not been something that we probably have paid a commensurate amount of attention to. I can say that and people will not like it, but I can't see that you can really argue with it. So we have tried to understand, first, who are the logical partners in this activity.

The three key pillars associated with the mission are the consequence management piece, which is, "Okay, you've failed at everything else, now it's time to clean up," which actually can be a deterrent, particularly against someone who is a terrorist or a martyr: if you take their objective away, you have a chance of affecting whether or not they decide to get up in the morning and strap bombs onto their body and go into a crowded place. If you remove that objective, if they can't get the effect they desire, you have a chance of affecting a terrorist. So it still is a very valuable weapon; it has deterrent value.

The other two pillars are probably more readily identified. Nonproliferation is that activity that says that the country you are dealing with agrees with you and wants help figuring out how to divest itself of anything that is of WMD class—they've seen the light, they've decided it's not appropriate.

Counterproliferation is more challenging. Here, you don't have a willing partner; you hope to develop a willing partnership with others to build an alliance that says, "This is just not the right way to do business, if you're going to continue on this path, then we would like to offer all types of deterrence to change your mind." But the two key pillars that were called out in our tasking in counterproliferation were elimination and interdiction. In those two areas, elimination is the idea, particularly in the course of conflict: you come across weapons of mass destruction, you have to have the capability, one, to isolate it—to "triage" the activity—and then move to an elimination activity, and the challenging part of this is when it's in the course of a conflict. So you're uncovering it as you move forward, you come across the cache, you say, "Oh, I've got this." You don't want to leave that front line unit there guarding it; you want to have a system that allows you to close, the technical experts recognize immediately what it is, then the triage activities—then people who know how to handle it as quickly as possible do, and we let fighting forces continue to fight. What we have not had in the past is a coherent command and control for that activity, the way to reach back and close, the technical skills along with the general purpose skills to isolate the area and then process it so it can be eliminated. That is what we're off to do.

We're working with forces that have been assigned in the 20th Support Group on the Army side that have the technical expertise. We're leveraging them for command and control and the breadth of, "How do I close the problem and set up the opportunity?" We've partnered them with the Defense Threat Reduction Agency, which is my component in this area because they have the technical skills. So by putting the operational skills together with the technical skills, building an overarching joint construct and then having that as a service that we provide to a regional combatant commander, a regional combatant commander deciding to prosecute some sort of a war plan or a contingency would then say, "Okay, there is some expectation that this could occur." We give them the cell for command and control; that cell has the inherent skills to reach back for technical expertise and the ability to discern, "What is it I just ran into? Is it a chemical, is it fissile, what am I dealing with here, what kind of experts do I need?" and then the lift and everything associated with closing the problem. It could be that we do this in conjunction with SOF [Special Operations

On March 22, 2007, Col David H. Gurney, USMC (Ret.), and Dr. Jeffrey D. Smotherman of *Joint Force Quarterly* interviewed General Cartwright at his Pentagon liaison office.

Forces]; it could be that we do it in conjunction with general purpose forces—it depends on the scenario. But that's the skill we're trying to develop.

The nonproliferation side of the equation is really where I would like to spend a lot of time, because nonproliferation represents that you've built the deterrent capability in your strategy and people are recognizing that it makes no sense to have these weapons; let's be partners and get rid of them. Most of that work heretofore has been done under Cooperative Threat Reduction in the Nunn-Lugar construct, which was really associated with the former Soviet states. We're in a dialogue now with Congress to understand how we can broaden this construct to a more global capability and start to allow regional combatant commanders to reach into this capability, to allow them to help their nation-states to help themselves: how do you build a border that can detect these things, how do you know in your country where this is, what's moving around, what got introduced that you didn't know about, how do you ask for help if you can't take care of it yourself, how do you interact with your neighbors in this activity, particularly if you start to think about bio[logical] problems, etcetera—and start to build these cooperative defensive capabilities that keep you from getting to elimination and having to worry about it in an uncooperative way. So we're trying to put a lot of effort into nonproliferation activities.

JFQ: *Do you have all the authorities and policy guidance now?*

General Cartwright: We've been given everything people can think of. But as we develop the CONOPS [concept of operations] and as we start to exercise, we'll start to understand where those authorities fall short. One area that we know already is habitual relationships in the interagency [community]. You don't want to put on the interagency process crisis decision activities; you'd like to set up and say, "Here's what we think are the range of activities associated with counterproliferation and nonproliferation," as an example, and "Here are the key actors that have to be working on a day-to-day basis in real-time." Our interface with the National Counterproliferation Center, our interface with the National Counterterrorism Center—that can't be only in a crisis, that's got to be a day-to-day thing, we've got to set up [the Department of] State as the lead for the PSI [Proliferation Security Initiative], which is a combination of the willing, so to speak. So we've got to have a relationship there because you don't want Defense to be something that's over here on the wall, and "break this glass if necessary," and by the time you do, the problem's already gone. So you have to have a day-to-day relationship. That's not standard in the way we do business in the interagency. We have JIATF [joint interagency task force]-type constructs, particularly in the [Department of] Homeland [Security]. This is similar to that, but it is day-to-day, what are the problems in the world, which ones are starting to bubble up and go in an adverse direction, what tools do we have to drive them in the other direction.

our interface with the National Counterproliferation Center, our interface with the National Counterterrorism Center—that can't be only in a crisis, that's got to be a day-to-day thing

You initially want to start with non-force-type tools, but if this doesn't go the right way, let's get the planning going right now about how we do it, who should do it, and what are the right authorities. Do you want to use a Justice authority, do you want to use an Intelligence authority, do you want to use a Title 10 authority? Maybe you want to use a different country because it's more appropriate, and that's what PSI lets you do: start to look cross-country and say, "Who's got the right authorities to match up to the problem?" And so doing that in a proactive way rather than a reactive way is what we've got to get to. That means we've got to have relationships in the interagency that are normally reserved only for OSD [Office of the Secretary of Defense] and the Joint Staff. We're trying to understand what those authorities are, what our left and right limits are so we stay in the boundaries, and we do subject ourselves to the appropriate oversight, but we also don't cut off the reaction times that we might need to go after something that could have a high regret factor—if we don't do this, a weapon is inside your border, or something like that—how do you start to understand, and that's part of the exercising, and the tabletop work is to get the interagency relationships right so that we don't violate checks and balances, we don't violate individual interagency head prerogatives, but yet we posture ourselves in a way that we can be successful.

JFQ: *Does the United States have adequate declaratory policy to deter new and emerging WMD threats, particularly with regard to potential rogue states' nuclear transfers to state and nonstate actors hostile to the United States and to a potential state actor's employment of nuclear weapons in an EMP* [electromagnetic pulse] *attack against the United States?*

General Cartwright: Declaratory policy is but one tool in a broad set of tools that go all the way from friendly interaction to kinetic force. Declaratory policy is like dealing with kids, saying, "Don't you dare do that or I'm going to spank you." That's appropriate at a certain level of behavior. What you'd like to do is set the conditions and the learning such that you don't get to declaratory policy. When do you need to invoke declaratory policy, when is it an appropriate tool, a critical activity? I'll take you back to the last question, because where I want to be dealing here is in nonproliferation and have that be successful so that we don't get to counterproliferation or to a case where we are going all the way, in a conventional sense, to phase II of a conflict where we're flowing force deterrent options out there to make them behave in a way that's appropriate and then coupling that with declaratory policy. So you'd really rather start a relationship based on, "Here's the way we think we ought to behave, here are the incentives to go in this direction, if you start to have inklings about going in a different direction, what's driving you there? What is it about your national security and sovereignty that you're uncomfortable with that drives you to a decision to have this capability? Can I do something about that? Can I do it early enough that you don't have to get to this point?"

If you get to this point and you start to posture, usually what we use is warning time in this scenario, so you get inside a certain amount of time where I can react if you act badly, you can react and surprise, now we're going to start posturing, and now we're working our way through an escalatory

chain in which there is a declaratory policy in which I tell you, "If you go any further, then I'm going to act in a certain way, and you can count on it." That should be a stick; I'd like to start with carrot, but if you force me to stick, this is the beginning of stick. So using it as a tool that you have for each of the countries is probably not the best use of declaratory policy. You'd really rather be working down here in nonproliferation, understanding what has driven that country to that, where do they want to end up, what can you do to help them help themselves go back to a position of comfort.

This is a campaign, this goes back to strategic communications, "Here's how we think it ought to go, we're starting to understand what's affecting you, why you believe what you do, it's either in our behavior or your behavior, but let's understand that, come to an agreement on it, and now what can we do to start to shape that in an appropriate way to get you more comfortable and us more comfortable." If I get to declaratory policy, that's in line with force deployment options and things like that. You're starting to posture, and you're way inside my comfort zone now. You've done something that I don't like, and it's making me nervous, and if you keep going in this direction, here's the stick that I'm going to hold.

JFQ: *Concerning your observation about the huge percentage of American businesses directly interfaced in a cyberworld and emerging cyber threats that are only 300 milliseconds away, is it necessary and possible for USSTRATCOM to influence changes in the architecture of the Internet?*

General Cartwright: The "Internet" is kind of a pseudonym for "networked environment," and the Internet tends to represent a more commercial application of the networks that has to do with information exchange, and generally, it's more social information. But networks at-large, whether commercial in nature, military in nature, governmental, etcetera, are where the bulk of American business is conducted, and they have huge implications in intellectual capital, people, in dollars and cents capital—on a daily basis, the transactions are huge.

They [networks] are global in nature; they tend to be self-policing to some extent, and the architecture is flexible enough that it will merge and morph in ways that protect it. But I'm going to give you two examples of, probably, the power and the unintended consequences side of this question. You go back to 1999, and a fellow in Saudi Arabia by the name of bin Laden is tossed out, and he goes to Afghanistan, and everybody goes, "Gee, bad guy, but what can he do from a cave?" At the same time, a student from Northeastern University by the name of [Shawn] Fanning is trying to figure out, "How can I use this peer-to-peer capability?" By most accounts, he takes around 25 percent of the music industry's profit in something called Napster. You can use this [technology] for good, or you can use this for bad; it depends on how you apply it. Do you change the architecture as a result of that? How do you treat this activity: as freedom of speech, or as a commodity that, when it crosses your border, you have the right to inspect? It all goes across the same kinds of pipes, it all gets intermixed. It doesn't pay much attention to geographic borders. Because of the Internet protocol activities, some of it may go through one country, and another part of the conversation or packet of information may go a different way—space, or someplace else. It goes extremely fast. So, "What is it and how do we treat it?" is a lot of the debate that's out there.

we probably erred on the conservative side to protect the use of the Net for everybody

I would say that we probably erred on the conservative side to protect the use of the Net for everybody. But let's equate that to the sea. When we did that on the sea, we tried to make sure that everybody could use the sea for commerce and have access and passage and a common set of rules, so we don't run into each other for the most part. But everybody had a right to be there, and we ensured that by creating a navy to have a presence on the sea. How do you look at this as an analogy—and is it a good analogy? Some of that debate is still going on, but you look at how the network has policed itself—in the case of Napster, in the case of intellectual property rights and how you treat them in the network—we haven't quite yet solved the problem of physical location. We've got some challenges in law because an American company operating on the network overseas has to be treated like it's an American company. Google, Yahoo!, MSN—those are American companies. If bin Laden wants to use them, he has every right to do it, and he's protected then by American law, not by Title 10. So how do these competing titles work in this network that just kind of throws all of that together in a hodge-podge? That's a challenge that's out there. But our principal activity is one of, when you talk about the architecture, is this is for Title 10 and for DOD [Department of Defense] and for STRATCOM, this is a weapons system. That helps us decide what the appropriate architecture is.

We have some advantages that the general business world won't have. If I tell Lance Corporal Cartwright, "You're not taking [your laptop] home, you're not plugging it in to those networks that are private, you're going to use this kind of a firewall, you're going to protect it in these ways, you're going to change your password, you're going to use some other type of identification or token," I can do that to Lance Corporal Cartwright. I'm not necessarily able to do that to the Cartwright on the street or in high school. And so what we're trying to do is stay inside the current construct, which says Homeland [DHS] is responsible for the United States Northern Command from a DOD standpoint.

When you start to spread out from the United States, then the layered defense capabilities belong to DOD, and we start to build a defense capability inside the United States, our bases, stations, places where we live are under DOD, so they are "dot-mil." We can start to have some control over it, we can standardize what's going on, we have the right to have a presence everywhere and know and see what's happening, so if there is a virus, or if there is an attack, or if there is exfiltration, we want to be able to start to register it, because we can be somewhat more intrusive on our military people than we can be on the general public. But what we're doing is building a domain that is more protected, so that when an attack occurs, we've got something to fall back on. Some of those practices are likely to be moved out to "dot-gov," and then "dot-edu," and on and on, to "dot-com." But they're probably going to be more driven by commercial practices.

My sense as an individual is that we hit that point in industry where they can no longer stand to absorb the losses of an attack while they wait for a patch and pass that financial burden on to the consumer. They are convinced they're going to have to be more aggressive about defending their networks and their intellectual property. That means there has to be a construct for the country. Usually what we try to do—this is the military—is to build a layered defense: get yourself out there far enough so that you can detect adversary activities that are coming toward you and have time to react. This millisecond thing is saying that from the other side of the world to this side of the world to that side of the world—it takes milliseconds. So how do we start to build a system in which we have presence in the littorals, so to speak, and out on the open sea or in the air, but really here in cyber[space]? How do you have a presence out there to see and know what is going on technically—how do you get yourself out there to the point where you can see at the speed of light what went by you, whether it was good or bad, report back, and reconfigure yourself for a defensive posture appropriate to that threat, before it gets there?

Those are the technologies that need to start to emerge both in the commercial sector and in the national security sector because that moves us from the idea of purely defending a terminal to registering the fact that there's a threat, doing something about it, and then deciding whether you want to take some action about it and acquiring attribution of who did this to you. That technology is where we've got to start to move to manage this medium in a way that is analogous to air, space, sea, etcetera, and thereby allow it to fit into the construct that we have, which is pretty much based in law, based on property, geographic boundaries, things like that.

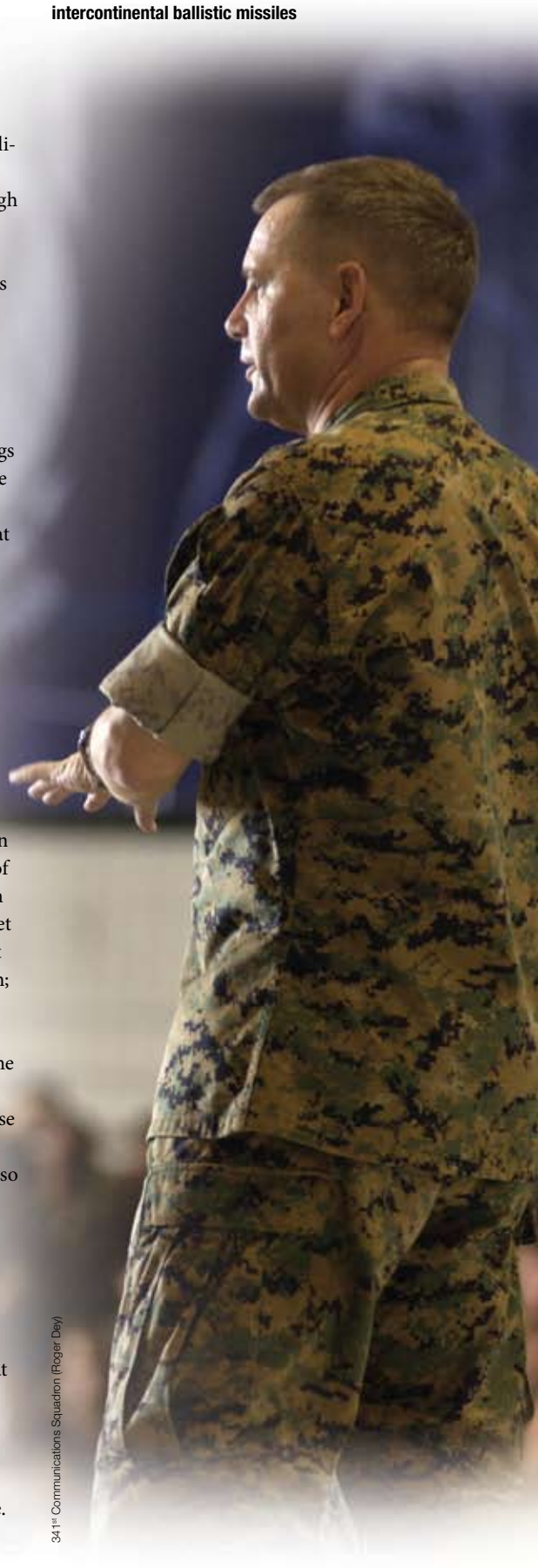
JFQ: *Building support for expensive military space programs is difficult when information about the space threat is shrouded in secrecy. How can we address the implications of the January 11, 2007, Chinese destruction of a weather satellite when we cannot easily communicate the enormity of the threat to the public?*

General Cartwright: In doing this in public fora, which we've done now in hearings and in the press, the activity is to forewarn, to understand that the Chinese have a defensive capability, a continuum capability that is a very deliberate plan on their part all the way from what we call temporary and reversible effects through this type of direct ascent, which is an expensive and forceful way of doing business, on up to more sophisticated and all the way to potentially nuclear capabilities to disrupt space and anything that flows through it. They're working their way through that continuum; they feel that's in their best interests.

To be fair, we've done this, the Russians have done this—we did this last in 1985, when we launched a direct ascent ASAT [antisatellite weapon] against a cooperative target. There are other things you get out of that: maneuvering guidance, navigation, the sophistication of boost, and all of those things start to come together; they [the Chinese] are on that same track. The difference here was, one, we had a couple of countries around that probably would have told you, "This doesn't make a lot of sense," and we abandoned it several years ago, as did the Russians, for a lot of good reasons. Two, if you're going to conduct those tests, there are collateral damages—the debris caused by such a test. The last test we did was in the 1985 time frame, and we did it down at the bottom of the belt of low Earth orbit, and we did it in a descending way, so that the debris would go down into the atmosphere and burn up. Even doing that, it was 2004 before the last piece of debris deorbited. So you're talking twentyish years for something that was optimized to get out of there quickly. Back then, there weren't quite as many assets in space. This is up high; it's going to have to migrate down through the International Space Station's altitude, it's going to have to migrate down through all the other parts of space, you're going to have to worry about it. If you want to—as the Chinese have said they want to do—go to the moon, you're going to have to go through this now, so manned flight is imperiled.

It's also a watershed event. You've now got another country that's decided to enter this activity, that, on the outside has said, "I don't want an arms race in space, I don't want to go to an armed space activity," and yet they're out there blowing things up. What should we do about that, what are the implications for United States space capabilities? Generally, the first question people ask us is if we need to go to an arms race. No, there's no reason to do that at this stage of the game. Just because you have a threat in space does

General Cartwright discusses the future of intercontinental ballistic missiles



341st Communications Squadron (Roger Dey)

not necessarily mean you have to address that threat in space. There are all sorts of other ways to get at that kind of a problem. When you go back to the continuum starting down at the nonkinetic stage, diplomatic activities and on up, there are plenty of ways to address that type of threat.

What we need to do now is to be more proactive in our situational awareness in space. Who's up there? We're going to have to have better awareness; we can't take a look at these things once a month and say, "It looks like it's okay, and the orbit is going to be in the same place when I go back again next month." There are too many objects now in the physical sense, and too much of the spectrum is used up in space, so interference in an electromagnetic way is also a problem. So we've got to become more proactive in that activity rather than just a cataloguing type of mindset.

Point two is, just going back to the analogy of the sea or air, the systems we put up there are going to have to be more aware of what's going on around them because you can't detect everything from Earth, and you want to be able to know that something's going on, having a sense of whether it's a natural phenomenon, or just a debris phenomenon, or whether it's something with intent. Usually it's electromagnetic in nature—people stealing time on cell phones, stealing entertainment channels—but piracy just like it occurs on land and in the air goes on up there. So we can start to build a collective awareness of what's going on in space. Those are the vectors that we need to be on.

JFQ: *A new National Space Policy was recently released in which uninhibited access to, or freedom of action in, space is a crucial prerequisite for all U.S. space activities. Realistically, can this policy be achieved when we are simultaneously committed to the peaceful use of space?*

what we need to do now is to be more proactive in our situational awareness in space

General Cartwright: Because we patrol the sea and have a presence there does not mean people can't get on it for peaceful purposes. It does not mean that if you have a border on the sea that you do not have rights to declare that border and treat it like any other border. Space shouldn't be any different. We should have the access, we should be able to operate up there to the extent that as the population goes up in space, so to speak, that we need rules like we have in driving, that we'll pass left to left or right to right, that we'll give each other a certain boundary of separation based on our ability to maneuver and see and perceive. Those ought to be brought in to ensure safe passage and somehow have to be enforced. It doesn't mean that you go up in space and you've got a little siren and a bubble light and you pull up, but it does mean that I'll call you if I sense that you're too close or if your spectrum is overlapping onto ours. But that doesn't mean that you go to space and you are a traffic cop or you have a weapon up there or something like that. I don't see those as being compelling activities that we need to move toward now. It's easy enough to call up two different owners in a spectrum dispute and say, "Somebody's stepping on the other guy. Go look at your health and maintenance data and see if your system is operating normally, and report back," and both of them say, "Yeah, we are," so somebody here is not working.

That's a lot easier than some of the other scenarios where, potentially, two parties build satellites. One is able to hold station physically in space better than the other, but they both have a slot that is X number of kilometers apart. If one is wandering around and can't be controlled, you're going to come to a decision that every time I turn around, I'm having to move mine because you're unable to hold station—those are the kinds of things that are likely to be harder to solve. What is the international body that we're going to use to have that conversation? How are we going to understand ground truths? Do we set standards before you go? If you violate standards once you're there and you put others at risk, how do we address that? We haven't gotten to a point yet where the activity is that driven, but you can see that that's going to happen, and it's no different than the naval example where you get, say, in straits, where it's got to be left to left, you've got to have a certain amount of distance because of maneuvering speed. We're not there yet, but you can see that's coming, both in the electromagnetic side and in the actual physical stationholding side.

I think we're moving in the right direction, we're probably moving as fast as the threat is emerging in that kind of a construct. There is money in space, there is commercial advantage in space, and usually when that happens, you have mischief. Thus far, it's been associated more with piracy-like activity of stealing signals, stealing bandwidth, potentially sliding into someone else's physical spot, something like that. You hope that that's

General Cartwright meets with Lieutenant General Robert J. Elder, Jr., USAF, Commander 8th Air Force

2d Communications Squadron (Sonya Padilla)

where it stays, but at some point, it could go differently. Those slots and that bandwidth are getting smaller and smaller, and they're in bigger demand, and the price is going up. Then you start creating haves and have-nots, and that's going to lead to some conflict eventually. We're not there yet, we're not even in a position, in my mind, where we need to posture ourselves for that kind of activity. We'd rather keep it at a low level, find the appropriate venue by which you can adjudicate those issues, and then do that down here on Earth.

JFQ: *Finally, sir, many in recent years have emphasized the critical importance of achieving unity of purpose and effort among diverse combatant commands and U.S. Government agencies and departments. How important is such cross-cutting collaboration for STRATCOM, and what are you doing to achieve it?*

General Cartwright: It's critical to us. Let me start first with kind of the emergence of global commands: TRANSCOM [U.S. Transportation Command], SOCOM [U.S. Special Operations Command], JFCOM [U.S. Joint Forces Command] to a certain extent, and STRATCOM, versus the geographic combatant commands. Each is unique, but the global commands tend to see things differently than a geographic command does. If you use a business analogy, the global commanders can provide scale to a problem but are not well positioned at the point of transaction in a business sense but at the point at which you interface with another country out there in a region. The geographic commander is going to have the nuance associated with a personal relationship, close observation, cultural expertise, etcetera, that a global commander won't have on a normal basis. So trying to provide him with the scale and breadth of capability that a global commander can bring to the table, and to move it to him when he needs it and to have it available for someone else when they need it, is more the model that we're trying to follow.

We're providing services of scale. Use intelligence, use space, use any of our mission areas. The geographic combatant commander has a certain amount of capability, but when things start to heat up, he's going to want to reach back for scale. He is still the best person positioned for the agility of day-to-day transactions and activities, whether that be in trying to defuse a crisis or in trying to defeat an adversary. What we're trying to do is provide in a service construct the ability to move scale to him for whatever objective he's trying to do, whether it's to defuse or to defeat. If we do it that way, that tends to keep the unity of command and unity of effort intact.

The challenge that's emerging today is that many of our sensors and capabilities are global in nature. Let's just take as an example the sensors associated with missile defense. Let's just use North Korea as an example, since we went through that with the Taepo Dong. If it launches from North Korea, that is a problem for USFK [United States Forces in Korea], but it immediately becomes a problem for PACOM [U.S. Pacific Command]. In its flight path, it will fly over Russia—that's EUCOM [U.S. European Command]. If NORTHCOM [U.S. Northern Command] decides the United States is threatened and decides to launch an interceptor, that's going to occur over Russia, and that's EUCOM again. So who's in charge? Who decides what sensors are aligned to that problem? Who decides when they're in maintenance and when they're being used? And some of those sensors belong to the Department of Defense, some belong to the Director of National Intelligence, some belong to other countries. How do you integrate that kind of activity?

The main kneejerk reaction was to give it to a global commander. But now you've taken a global commander who is not at the point of transaction of any of those things and inserted him into that activity. Our approach is to provide each one of them with the situation awareness they need for the function they're performing. If they're managing sensors, the launch of the vehicles, the basing, if they're the source of the attack, they need to know certain things to be able to function.

slots and bandwidth are getting smaller and smaller, and they're in bigger demand, and the price is going up

Build a command and control system that gives them that awareness, but don't rush to centralization of the activity. Try to find a tactical and command and control relationship that allows each of them to perform their function inside their area of regard.

The missile defense system was not initially designed that way. It was designed to have one person in charge, and their belief was that it was the person being attacked who ought to be in control. But is that where you're going to fight, or is the fight going to occur at the point where it [the attack] was initiated? What about this guy that was a third party and had a weapon of mass destruction destroyed over his head? So how are we going to do this? This is a big challenge. Our belief, though, is that the technology is there to devolve this down as far as you can to the person who is at the scene. Make them the strategic corporal; give them the tools to do what they need to do at that level. If there needs to be integration across this global activity that just crossed nine time zones and four combatant commanders, okay; provide the tool set and the CONOPS to work in that environment, but don't just take the control and centralize it immediately. It doesn't serve us well; it doesn't give us the agility at the point of activity that we're going to want to have. We did that, and we do that, at STRATCOM with nuclear weapons, but that's a little bit different in the regret factor, number one, and number two, the idea here is that we don't want to have to use those things. If somebody attacks you, you want to be able to defend yourself immediately, you don't want to negotiate that; self-defense is not negotiable. Much of command and control ought to put us in the mode of being able to do this work and not have to be in negotiation for the guy that's affected. You've got to be able to disperse this in a way that makes sense.

That's what that command and control system has got to bring to the table. But the guy who can best decide what to do is the guy at the site. That's the way we've got to design the system. Are we there technically? Technically, I think we've got it. Culturally, I think we've got to work our way through this—CONOPS, things like that, are just not ready for that kind of sophistication, but they're getting there. I believe that over the last year, the commands have come a long way in understanding how they can get their equities addressed and preserve unity of command in their AOR [area of responsibility], where they're responsible and accountable for the activities.

JFQ: *Thank you, sir.*