

**CENTER FOR
STRATEGIC AND INTERNATIONAL STUDIES (CSIS)**

**2010 GLOBAL SECURITY FORUM: HOW TO STIGMATIZE THE
USE OF CYBER AND ANTI-SATELLITE ATTACK?**

**WELCOME/MODERATOR:
JOHN HAMRE,
PRESIDENT & CEO,
CSIS**

**SPEAKERS:
GEN. (RET.) RON FOGLEMAN,
FORMER CHIEF OF STAFF, AIR FORCE,
U.S. JOINT CHIEFS OF STAFF**

**JEFFREY HARRIS,
CORPORATE VICE PRESIDENT,
MANAGING DIRECTOR, SITUATIONAL AWARENESS,
LOCKHEED MARTIN**

**LT. GEN. (RET.) MIKE HAMEL,
SENIOR VICE PRESIDENT OF STRATEGY AND DEVELOPMENT,
ORBITAL SCIENCES CORPORATION**

**THURSDAY, MAY 13, 2010
9:10 A.M.
WASHINGTON, D.C.**

*Transcript by
Federal News Service
Washington, D.C.*

JOHN HAMRE: We're actually going to start a little bit early because we've got too much to talk about. This is probably one of the most interesting topics of the entire symposium.

(Off-side conversation.)

MR. HAMRE: Welcome. Thank you all. This is going to be, I think, one of the most interesting topics of the symposium because it's an issue where we really have unresolved policy space. I think ever since the day that the Chinese destroyed a satellite in orbit, it shifted a lot of people's thinking. And we have been doing a lot of changed thinking here that we've obviously had a declaratory policy that for many years was grounded on the fact we had such a dominant control of space. And that's now evolving, and evolving in somewhat unpredictable ways.

Now, we are very, very fortunate to have this panel. I have had the privilege of working with Ron Fogleman for many years. We continue to serve together on the MITRE board. But Ron was also the lead general officer who was helping with the so-called Schriever series. And that, of course, was a path-breaking series of inquiries into the nature of space, space assets, space vulnerabilities, et cetera. And he has done more to shape my thinking than anyone in Washington. And so I'm very grateful that he's here and we're going to start with Ron.

Jeff Harris, of course, was the assistant secretary in the Air Force. He had the responsibility – he was managing the NRO. He is a guy that's been in and around space more than any other civilian that I know, and really shaped much of the current landscape that we have in the space community. So Jeff, we're delighted to have you here. And Mike Hamel, everyone knows Mike Hamel as being kind of one of the quintessential intellects that the Air Force has had and that the department has had on space policy through the years. Truly a practitioner and expert in every domain.

So it's going to be a fascinating discussion and I'm going to simply try to stay a little bit – hold us together – these three horsemen here of the apocalypse, we will try to hold them together a little bit. And then of course draw all of you into this conversation because the quality of this discussion is really going to be very much driven by the quality that you bring to it with your questions. So Ron, let's start with you and why don't you get things started?

GEN. (RET.) RONALD R. FOGLEMAN: Okay. First of all, it's a real pleasure to be here. And as John said, over the last eight or nine years, I've been involved with the Schriever wargaming series, which has really shaped a lot of my thinking on the subject.

John was very kind – he kind of glossed over how it was I was associated with that. I was a senior mentor, okay – an explosive term in this community – (laughter) – and this town. But I would tell you that it was worth the article in USA Today to be described as a senior mentor to also have a New York Times reporter declare that I was a military industrial legend.

(Laughter.) So I have put that on my calling card and increased my rates. (Laughter.) John, I'll tip you off here, but.

Now, the fact of the matter is the Schriever wargaming started out – and I'll just – the first game back there in 2001 was really kind of looking at things like space control, counterspace, adversary capabilities, which if you break them down, you're really kind of talking about where are we on vulnerabilities.

There was very little but some discussion about commercial space in those days and there was a lot of recognition that it was important to look at this area because it really did have global implications not only from a military perspective but commercial as we went forward. All of this fed into the requirements and capability thing. Over time, one of the most significant things that we did out at Schriever is we introduced allied participation in the form of Australians, Canadians and folks from the U.K.

And the first thing we discovered after we got them all spun up and brought them out for the wargame was we couldn't tell them anything and they couldn't tell us anything. And amazingly enough, we went to work on that. And over time, we have actually come up with a construct that makes the allied participation very meaningful and quite insightful.

We went down the road then, looking at the objectives of later games. We got into Schriever 4, which occurred in 2008, I think – 2009, perhaps – looking at how to defend and replenish on orbit. We looked at command-and-control relations between functional commands like STRATCOM and regional commands, the warfighters. We started to look at how national space policy might evolve, and looking at alternative concepts.

By the time we got done with Schriever 3, we were at a point where maybe egotistically or maybe because we were all wearing uniforms, we pretty much came to the conclusion that the uniformed guys understood this – and this is where I started interfacing with John – because the problem was we think we – to the extent that we have the tools to do observation, classification, situation awareness, the problem was when you started to try and hand this off to the policymakers in Washington, it didn't appear to us as though they were very well-prepared or very much in the game.

For instance, in the game prior to the last one, we were so desperate to get a policy perspective on this, as the senior mentor, I ended up being the chairman of the Joint Chiefs, secretary of defense, head of the National Security Council and the president. And I'll tell you what, that's a pretty streamlined chain of command. (Laughter.) You can make decisions, you know? (Snaps fingers.) Things happen.

But in a wargame, you have to be able to keep the game going and at the same time, though, get some deliberate play. And that's where Dr. Hamre then came in because we were having trouble getting serious participation, and so I went to him. He used his network, we brought people to town, we talked about it, and then in the last wargame, we had a whole different environment. And I think it made a big difference because we had a former

congressman who was involved in space playing the president, we had a couple ambassadors who were involved with space policy and these kinds of things actually role-playing.

So what are, then, the pronouncements that come out of all this? And I'll close up and go from there. I think one of the greatest lessons that we learned is that attribution for anything that occurs in space is really tough. It's really tough. And it's tougher if you don't have situation awareness. Now, why is attribution important?

It's important because without attribution, the senior command officials or the national command authorities will be very reluctant to act. The first question is, how do you know it was XYZ who did it? And this is in an environment in which decisions cannot be made in days if you're talking about doing things to protect assets, et cetera, and so attribution is very important.

And along with that is the potential – and Gen. Cartwright alluded to this somewhat – that we are actually being anesthetized over time by disruptions and anomalies that are being introduced by potential adversaries, et cetera. Fourth item: Allies must be a part of the solution. And this is not just something that we picked up on as we look at this evolving national space policy that says there are so many people involved now that we cannot do this unilaterally. Even if we could afford it, we couldn't do it unilaterally. But it does introduce a whole range of issues.

How do you define who an ally is in space? How do we want to define that? I think it's wide open. And we may not want to be as exclusionary as we have been in the past. Security issues and sharing of information becomes a real challenge. And then as you move towards this national space policy that includes allies – commercial and others – is how dependent can we afford to become?

And I think what's evolving here is something that says, we may have some crown jewels that we and anybody that's out there in space will always want to try to protect. And we can probably afford to do that. But in the main, it's going to be in everybody's best interest if we do more sharing of assets – again, both national, in the sense of the government, and commercial.

The next is commercial space is already a vital part of the military space capability. It's not going to change. It's only going to grow in capability. The issues that we have to sort through here are, what is the true cost not only in dollars to get this capability as an adjunct to commercial but what is the cost in terms of risk management, availability, et cetera?

The next-to-the-last item I have is the impact of ITAR policies. It was very enlightening for us to discover in one of our wargames that because so much of the satellite construction now has gone offshore and the companies who are manufacturing these satellites and their customers tie up this capability in a way that if you have some kind of catastrophic event in space that starts to decrease the U.S. capability and you want to go buy capability, you may find yourself in a situation where the commercial manufacturers, the commercial operators, have agreements with folks that you would not necessarily like to have controlling this thing.

But this is a business endeavor; that's the way things work. So this whole idea of the ITAR impact, while very difficult for the history major to really get involved and describe, is absolutely on one level, I think, impacting industry; on another level, we hadn't even thought about the hidden dangers in this.

And finally, my last point would be that deterrence in both cyber and in space is longer a unilateral U.S. action. We cannot build, in my view, we cannot have – we can have a declaratory policy, we can have a lot of things, but it is not going to be effective if it is the U.S. only.

Dr. Hamre referred to the Chinese satellite shoot-down. I think what you saw there was a nation that reacted not to a unilateral kind of complaint but an international complaint. And so I think that both in cyber and in space, deterrence has got to be built on us defining some sort of international norms that people have agreed to, and then as a community, police people who step over the line. With that, I'll stop.

MR. HAMRE: Thank you. Jeff, let's turn to you.

JEFFREY K. HARRIS: We'll go on a journey this morning and we'll hope that the journeys can try and define some of the dirt roads that we wrestle with. If you consider Benjamin Franklin in his role as the U.S. government representative to the French court, when he started in 1776, he was in Paris to attract a partner for the American rebellion. The colonies were without money, munitions, credit; there was a need for deterrence.

Here, Franklin, the best orator in Congress, was embarked on a journey. He was industrious, crafty, patient. Spying was universally rampant. There was lots of opinion but not much information, and quite frankly, lots of disinformation. Attribution of facts about the colonies was nonexistent. Information traveled by ship. Time was a different commodity than today.

Looking at the collection of archives, thankful to the interceptions of the spies, we now know what the French wanted the British to think; the Spanish tell us what the French really thought; and the French archives outline what the French ministers discussed amongst themselves.

Then we have all of this put together into the construct of, we now know how it turned out. So French helped fund the war; following victory with the Americans; the British wanted peace and reconciliation; the French wanted an alliance and a war. Setting aside religious debate, typical conflict was and is defined by ownership of things, places and requires visibly capturing the flag.

If I now fast-forward 230-some years, the speed and influence of information has fundamentally changed the speed of society and influenced the demands made on society by the governments. This effective shrinking of the globe, combined with the numerous non-state actors in global governance and commerce, is profoundly influencing the construction and implementation of deterrence policy in the related actions.

Now, most of us, as I look around the room, grew up with the construct of mutually assured destruction and how calming that was – (laughter) – as the prima facie evidence that any significant escalation to war threatened the existence of the planet. (Laughter.) Knowing what I know today about technology and recalling crawling under my desk in third grade, I find it just a tad incongruous. But the fear of nuclear exchange drove numerous aligned behaviors and policies nation-state-to-nation-state, in or out of the nuclear club, and restricted access to nuclear technologies by non-state actors.

Our session today will discuss the lever arm of deterrence policy, as affected by two closely aligned technologies – space and cyber – as we search for a magic elixir of invincibility. As a technologist, I've helped to nurture the space and information technologies along and have watched the societal behaviors, norms and perceptions change.

Consider the double-click, easy availability of satellite imagery today and how it contributes to transparency. You know, as we were putting together space imaging, the number of people that wanted to allow their faces to be imaged every time they do an ATM transaction, but did not want highways, cities and byways imaged was always sort of a curious construct of privacy, because the only difference was cameras up close were fine and cameras in space were bad.

So when we talk about deterrence policy, you have to put it into the context of what capability that we're talking about. So as a result, the combination of the technology and the political shrinking of the globe with increased entanglement – typically economic – and the speedy information, the utility and the effectiveness of the deterrence lever arm must evolve and change.

So let's look at space: 50 years ago, we were just trying to figure out how to make it all work. We matured the technology that now allows instantaneous global communications, weather surveillance, reconnaissance, navigation. We take it as a given utility. Shortly after we invented the technology, which is interesting, we started to invent the framework to govern it.

In 1967, several parties signed up to the Outer Space Treaty for the peaceful benefit, interest of all countries not to put nuclear weapons there; responsibility – states shall be liable for damages caused by their space objects; and that states shall avoid harmful contamination. So pretty insightful, going all the way back to 1967, as we got to this new ocean, to think about how it all fit together.

So to go back to Gen. Cartwright this morning, the space-faring states that are in the club have operated freely and responsibly to collect and disseminate information and avoided any weaponization of space as an operating theater. It's just that the club now has more members. So if you'll look back to the decades as I was growing up in this industry and in theater, space was always a place – a place that contributed to military capability – but was not “the” capability or “the” place to conduct war.

So we kept talking about the things and the platforms and less about the capability. And back to Gen. Cartwright this morning. He's talking now more about the capability and the

integration of capabilities. As a result, space the place was not perceived as the military contested environment. If you had to militarily deal with denying an adversary's capability, activities such as jamming were considered within the military norms.

All was good until along comes the World Wide Web. So when you're late for somebody's birthday that you care deeply about, you go out and spend \$3.95 on a card that plays "Happy Birthday." That card has more computational power in it than the country had in 1950. (Laughter.) So a lot changes with this thing called Moore's Law. Modern computers combined with fast telecommunications have come together to give us discriminating power at the tip of our fingers.

This peaceful endeavor to connect the citizens of the world together for industrial and academia pursuits has a profound impact on our economy, how we provide goods and services, and it increasingly challenges the jurisdictions of nation-states that have been challenged in their more typical and traditional regulatory regimes.

Think taxation; think the nation-state filtering of content. This rapid advance of technology is clearly outpacing the wisdom of committees responsible for governance. After Estonia and the Republic of Georgia, the world saw how a nation-state might use denial of service against nation-state computers as an enabling step in the preparation of a battlefield.

So with today's economies of the world having such a great dependency on the capabilities provided by satellites and the digital global fabric of the World Wide Web, I'll contend that space and fiber are merging and aligning where they are seemingly inseparable. So what is curious is that for decades the barrier to entry to space was lots of smart people and money, or lots of money and a few smart people, where the barrier for cyber is much, much lower, both in money and in people.

So following the Russian hacktivist incidents, the policy community is challenged with how to treat the noncombatant cyber-patriot who is beyond control of the nation-state. So the asymmetric nature of the threat, its potential significance of the implications, challenge us to align thinking so that we might best manage this global commons, managing complex government across international, civil, federal, private, where space and cyber must align and where attribution to assign responsibility for any misdeed would challenge even the best Sherlock Holmes.

So just when you think you have figured this out, imagine thousands of Geek Squad technicians in their Volkswagens with their pocket protectors providing ground truth about attribution in a quickly escalating conflict. This must put some fear in the seasoned policymaker, but this is where space meets cyber.

So the JCS pub clearly defines deterrence and if you look at it as the credible threat of unacceptable counteraction, it's clear that we should not treat space as the place or cyber as the broad word of cyber.

So the five steps of new deterrence: Moving beyond nation-state and kinetic, we must understand the operational capability nuances about the adversaries in short timelines previously thought unthinkable. Adversaries that are non-state actors can quickly form coalitions.

Two, we must inform the global collective that space and cyber are foundational elements of a nation-state's power. Although space and cyber are outside of a traditional territorial boundary, they are essential ingredients in implementing national power.

Three, space and cyber, although relatively new, are conceptually old. Perhaps these are the new territories of oceans and rivers; freedom of navigation and freedom of passage.

Four, compressed decision time with attribution ambiguity make military and policy triggers much less clear. Get used to red lines that are ambiguous or substantially redefined red lines on how you intend for them to shape adversary behavior. There is a need for the adversary to understand that they are to be held accountable for collateral damage and unintended consequences. If you think unintended consequences are challenging here, ponder where we go next with the biologic threat spectrum.

Five, industrial age policies, processes, organizational constructs, must evolve for us to successfully manage information age conflict. Informations follow Moore's Law; so must acquisition. People, process and technology is changing faster than the system that we ask all of those three modalities to perform in.

So in summary, the speed capability of today's information systems is truly a great enabler for the citizens of the planet. We will always face conflicts between the haves and the have-nots. I am confident that the increased transparency and the educated, informed citizens that information systems provide can help advance potential for peaceful, global governance.

We have a renewed emphasis on space and cyber situational awareness. This provides important insights about what is and what is not going on with what will be a technological cat and mouse game for supremacy, military and economic. As we learn from Franklin, there is information and there is disinformation. As we now are all actors on the connected world stage, the leaders will best be able to use information or the perception of truth to drive deterrence thinking. Thank you.

MR. HAMRE: Jeff, thanks. Ron and Jeff have certainly raised all the questions. Mike, why don't you answer them? (Laughter.)

LT. GEN. (RET.) MIKE HAMEL: Thank you very much, Dr. Hamre. First of all, I think is an extraordinarily important topic and I'm very pleased and commend CSIS and your personal leadership, sir, for bringing this to the forefront. And I feel very honored and humbled to be part of this distinguished panel.

This obviously is a very complex and challenging set of questions. And if anything, the events of the past several years – the Chinese ASAT tests, the collision of the Cosmos satellite and the Iridium satellite on orbit, reported jamming and disruptions, both against international as

well as domestic capabilities – has certainly elevated the import and helped frame these questions in ways that we perhaps hadn't been thinking about for some time.

I'm going to start off my thoughts here by noting that most of the purposes, capabilities and organizations and the way in which we have approached space largely have their roots in the Cold War superpower competition. And what really has happened, though somewhat unnoticed over the past decade-and-a-half since the demise of the Soviet Union, is that space now has become inextricably woven into civil society, international affairs and commerce, and probably more pointedly, the way in which our U.S. military today actually operates.

The fact of the matter is, is that our national strategy is one that depends upon being able to have global knowledge, awareness, the ability to act at times and places sometimes not of our choosing. It underpins our strategy and it enables such capabilities as precision warfare, expeditionary operations; light, lean and lethal combat, and in many cases, such things as even humanitarian relief as well as dealing with natural disasters.

So what I would suggest here is what we're now grappling with today is that this now has become, if you will, the free access and use of space for us has now become a vital interest for the nation. But it is one in which we have becoming increasingly dependent that is also operating in a relatively open environment and domain and that is now becoming increasingly an inviting target. And the fact of the matter is, is that presents significant incentives for others out there to perhaps threaten to be able to level the playing field or, in some cases, actually harm our nation.

So I think that what we're really dealing with here is the necessity to rethink our interests and approaches in space from the perspective of the 21st century. That is one where we are a multipolar world that is highly interconnected and globalized across all dimensions, whether that be political, military, economic. And that what we really have to be able to do is to found our activities, if you will, on enduring principles that will obtain in the 21st century. So let me just offer a few things here in terms of what I think are some of the foundations of what I would characterize as our space security and defense for the 21st century.

First of all, again, we have struggled with many of the issues throughout the Cold War and, frankly, we have got some very polarizing as well as contentious argumentation. All that we have to do is to think about the great raging debates over weaponization of space. We talk about what the benefits are or perhaps arms control limitations relative to space. Even our rhetoric where we talk about we want to have a posture and a strategy of space dominance and superiority oftentimes tend to be polarizing and does not really get to the heart of what's at stake here.

Refreshingly, I do see an increased debate and dialogue today in terms of what should be our future course. We do talk about such things as deterrence and dissuasion. We talk about pursuing international norms and rules of the road that can create a common interest and understanding.

I would suggest, though, that what we really do need to do is to start from some very foundational first principles. And that is that the fundamental responsibility of any nation – and it's both a right as well as a responsibility – is to defend its territory, its citizens, its sovereign assets and interests, to honor its international commitments and, if necessary, by all means, including military force, to ensure that its interests are upheld.

We also see now an acceptance that space really is a global commons and that we respect the right of all nations to operate in space for legitimate purposes. We likewise support the idea and the premise that space should be for peaceful uses. In fact, the United States is party and has been for many decades to a number of international agreements wherein we agree to a particular behavior, such as how we actually operate in particular locations, use of spectrum, recognizing practices of sovereignty and recognition of liability. So in some fashion here, we already are a party to a number of international norms, most of which people would agree have not really limited our actions and interests in any particular significant way.

I think another key first principle is, is that the real seed of purpose for what it is we do in space is not in space itself, but rather what effects are actually delivered on Earth here. Satellites are simply a means to an end, whether that be security, science or commerce. And we need to really focus on what the effects and the intents are of what space capabilities deliver on Earth to really – to guide our activities, as well as how it is we view the purposes of these things.

And I think that the other point here is that we must be able to look at space as a domain in which we have to be able to exercise our legitimate rights and likewise, to ensure that others do not impinge and infringe upon those particular rights. So let me suggest that I think there are several different elements of what I believe needs to be a layered strategy as we go forward to truly be able to protect our interests as well as to shape the environment for the future.

First one I would suggest is, is that we really need to get into a posture where we're engaging, cooperating and becoming much more interdependent with our friends and allies. And I would say that there really is several layers of this. One has to do with those that truly are our allies – longstanding relationships for which we share common interests. But then there are also going to be partners out there, those we share economic or business interests or coalitions with.

The fact is, is that we have a number of existing relationships, whether that be as intelligence relationships to our commercial practices as well as our international cooperative space relationships that can serve as a common foundation for much of this. The fact is, though, that part of sharing that common interest is also being willing to share our capabilities. And I think that is going to be a key part, as Gen. Cartwright spoke this morning, that we have to be able and willing to share what we have, but also then depend upon what others can bring that can actually strengthen our posture.

I think a second key point is it is going to be critical to extend the norms and rules of the road by which we actually operate in space. And those need to be consistent with our interests and those of our allies, friends and partners. Again, many of the things that we have spoken about, such things as the right of free passage, the inherent rights of self-defense and collective

defense, defense of citizenry and our sovereign interests, but also such things as acknowledging that there should not be interference with other's uses of space other than in times of conflict.

And likewise is that there should be avoidance of actions that could actually harm the free access and use of space. Creation of longstanding debris is one of those that I think the – clearly, as the topic of this panel of stigmatizing – I think that was clearly one of the lessons that came from the Chinese ASAT tests, is that the nations of the world cannot tolerate that kind of behavior.

But we also need to understand that should things come to pass where we actually do get to the precipice of conflict or armed conflict in space, that we need to apply the normal rules, the customary practices that we see in the law of armed conflict and the use of rules of engagement that create some measure of transparency and understanding.

We need to understand what constitute hostile acts and intents in space. We need to understand what the rules of neutrality are and what are considered combatants in a conflict. We need to be able to apply rules as well as customary norms in terms of what are proportional responses and what should be the defended assets involved in a conflict.

I will say in terms of a kind of third element of the overall layered strategy is, is that we must reduce the vulnerability of our own systems and capabilities and to leverage our technological superiority and advantage, if you will. The fact of the matter is, is that we have built constellations and capabilities for peaceful, peacetime uses. And quite frankly, they are ill-prepared to deal with the kinds of conflicts and threats that we may face in times of conflict, all the way from interference and disruption on the ground to actual physical vulnerability on orbit.

I would say there are things that we can do in terms of application of our technological advantage, whether that be improving our space situational awareness, and as was suggested earlier today, of how it is we can actually leverage our unique abilities to be able to bring together systems of systems in ways in which not the individual satellites, but rather, how the systems indeed will create a greater advantage on the ground needs to be part of that.

I think the final point I would make relative to a part of the layered strategy is, we simply have to become more open and vocal about how we interpret and what kind of declarative statements we make relative to how we envision and would interpret the use of space, not only by ourselves, but also by our would-be allies, friends, as well as adversaries. I think it is critical that we start developing what we consider to be redlines – that is, things that will create clarity in terms of how they will be interpreted by the U.S., as well as how we will hold others accountable for actions that they might take.

Interestingly, during the Cold War, we had a very accepted regime that said neither side would do anything that disrupts the ability to detect attack or to be able to command and control the nuclear forces on either side, which were a critical enabler of maintaining the stability in the nuclear deterrence during the Cold War. I think such kind of understandings and declarative policies would go a long ways in creating the kind of regimes that would help to preserve our

interests and capabilities in space, at the same time creating transparency and stability with friends and allies, as well as with would-be adversaries.

So let me kind of close off here that I think that the posed question here for the panel about stigmatizing ASATs, I think, is just but one of many, many different aspects of how we need to create the right kind of regime for how we will in the 21st century work with friends and allies as well as preserve U.S.'s advantages.

The fact of the matter is that one of the things I worry a great deal about is we might talk ourselves into a position where we view space as being too vulnerable, too costly, that we simply can't depend upon it, which I think would be a very unfortunate circumstance because of the degree to which space now has become a critical enabler as well as a point of our continued ability to act on the global stage and be a world leader in both security as well as defense affairs. So I thank you very much.

MR. HAMRE: Mike, thank you. All three of you, these were really, very insightful presentations. I learned a lot listening to you. Each of you, in your own way, has described a central problem.

I mean, there are classes of problems in the world that can be defined, but they can never be solved – murder, adultery – you know, the classes of problems that all societies object to and find abhorrent, and yet, they can't be solved. So they have to be managed and we establish structures to manage them.

We create laws to stigmatize behavior that's abhorrent to society. We establish some deterrent structures, legal structures, prisons, et cetera, to put enforcement to it. It still never solves the problem. And I think we – each of you, in your own way, have been describing, we have this kind of a problem.

And I'm going to start with Jeff, but I'm going to actually take it to the other three of you to say that we have – what's unique about cyber and space is that warfare in these domains have no strategic warning – very hard.

And so since we have to think of a system that now is managing this problem, stigmatizing bad behavior inside this, what would be the one thing – we can have two if you want – one thing that you would want the president and the National Security Council to do during the next year that would start us down the road to manage this problem? Jeff, let me start with you, and then I'll turn to Ron and to Mike.

MR. HARRIS: All of us this morning have spoken to attribution. And if you're going to operate in a set of norms, you have to have some expectation that those norms are going to be enforced. Cyber is the clear example that we tolerate others on our networks every day without either enforcement or attribution, whether it's cyber crime for money from syndicates or it's the theft of intellectual capital to allow, it's been estimated, \$40 trillion of downloaded intellectual property out of the United States last year. You have to set some line in the sand in order to stop that. So the number of people being held responsible for crossing the line of societal norms has

to change as we evolve from, you know, the Wild West to more ordered societies. I think as you do that, it causes people's behaviors to change.

My guess is, normal criminals watching CSIS, understanding the power of DNA in a courtroom in order to have attribution will allow the evolution of the criminal element. The nuance of the attack in space or cyber with improved situational awareness will allow us, I think, to raise the bar on behavior.

MR. HAMRE: Mike?

LT. GEN. HAMEL: Yes, sir. I would agree with Jeff on one point, but if I'll take also your opportunity to maybe raise a second one. First of all, I do think that our current inability to really understand what is happening in space is a real crisis. The fact of the ambiguity, where you're presented with circumstances where you really don't understand what exactly it was, what the intent, whether it was natural or hostile, is an extraordinary vulnerability that we have.

But I think the real point though is that the solution to that is not just simply inventing more programs or throwing more money at it, but there really has to be much more of an engagement and cooperative environment out there, not just – both within our own agencies within the government, but also with friends and allies around the world.

So I would say in terms of what is it that our national leadership could do, I think one is we do have to improve our capability. But I think the way in which you do that is through an engagement and a cooperative kind of – both within the U.S. as well as with friends and allies.

GEN. FOGLEMAN: Well, I think the first thing that I would really like to propose is that we would put in place a process that will lead to a clear set of rules of the road. And I think that's not a very easy thing to do in 18 months.

But the first place you start is with a domestic effort and then once you are pretty well squared away and have some kind of concurrence, assuming you can do that in this diverse community, you have to take it to the international community and so then you have a clear set of norms upon which you can build a declaratory policy. I think the sooner we can get a declaratory policy out there, the better off we are, both in cyber and in space deterrence.

Concurrent with that, I would pick up on Mike's point which is, it's all well and good to understand the rules of the road, the norms, both from a domestic and international perspective, but if you are clueless about what is really happening, then it's not nearly as effective. So we have to continue this effort to improve our situation awareness. And clearly, this is something that is best done, again, I think, in a collaborative effort in the international community; that is, we exchange information in terms of what we know about what is happening with consultations.

MR. HAMRE: Ron, you, in your remarks, mentioned the international – well, everybody mentioned the national dimension but you specifically mentioned and used the word "ITAR." I think ITAR is a shorthand for a much more complex landscape.

We have a mentality in this country: Everything that's good is in this country and everything that's threatening is outside of this country and we've got to isolate ourselves from them and keep it contained. And of course, space is a world that's evolved so dramatically, at least in the last years. Nothing probably more vividly shows the parochialism of America's policies and our inflexibility to respond and the way it's affecting us. And yet it enjoys this superior idea that somehow, fear is a strategy of security.

So what do we do about this? Because we've got to transform the way we think about industrial security because it's – what our current policies are doing are effectively creating an enclave for competitors to get better than us. So what do we do? Ron, you started this, and then I'm going to turn to our colleagues to jump in.

GEN. FOGLEMAN: Well, I think the difficulty in this area is on the one hand, we have a world out there in which from a cyber dimension, our intellectual property is being stolen and flowing offshore at a horrendous rate and at the same, then, you need to, as senior policy people, be able to stand up and say, yes, this is happening and we're working on how we can best defend against that.

But at the same time, you're then advocating sharing things, which has always seemed to be the problem. My sense is that we're past this from – whether it's this administration or another administration, I think we have now recognized that this is such an issue that we're kind of past it from a State, Commerce, OSD perspective. We want to get on with doing something differently.

I think our big problem here is going to be how do we convince the folks in the Congress that this is truly a problem that is creating enclaves for other people in the other part of the world to basically develop and sell capabilities that our industry is not able to do? That's part of it.

But more importantly, if you go back and look at what has given us the – why we have for so many years had such exquisite capability in space, I think it was because of people like Jeff and others in the NRO and other agencies like Mike ran, where we were always able to stay about two generations ahead of anybody else with technology. That was the thing.

Staying two generations ahead, in my view, provided far more capability to us than protecting that one-generation-old capability. So we have now tried to protect it all and as a result, we're losing because to stay two generations ahead, you have to have investment. You have to be able to do these kinds of things. I think that's one of the arguments we have to make as we go to the Hill.

MR. HARRIS: Forcing technology to follow the old mold of policy and legal framework, I think, has failed. As Dr. Hamre pointed out, we have a borderless situation here with both cyber and space. We have a country that was founded on personal privacy as something that we want to protect all the time but we have to get Americans to understand – back to my ATM camera example – where does your personal privacy start and stop and where the societal needs for societal control start and stop.

So the fact that I can be a teenager and horsing around one night and it's to my advantage to horse around near the county line or the town line because the police can't pursue me two blocks over – to have, over the last couple decades, those laws to be softened about the right kinds of pursuits and the right speeds of pursuits in order to protect the balance of the individual and the balance of society.

Fast-forwarding now as I move from one server to another, in a logical space, I am constrained by an awful lot of geographical physical thinking, and so forcing this technology to sign up that way is hard.

Gen. Fogleman's comment about the need for us to run fast in technology certainly differentiated with us with the very successful outcome of the Cold War. Again, I want to take that same "running fast" on technology and say, double down, let's run fast on the policies to keep up with that.

And so certainly, forums like this that allow us to educate the people as to how to think about it – I have long advocated that we should start about sixth grade a national effort on what I'll call "cyber hygiene": an understanding for all of us, as citizens of the world, to understand what are the appropriate norms as a child growing up because we're proficient at age three or four to move the mouse and cause the computer to do stuff. As I get to where I add logic to that, to the necessary building blocks and ingredients, I can align the "run fast" together.

The framework that we have to operate in is to get us to an environment where we recognize that smartly thinking about all of this is really important. I think in this cat-and-mouse of any times you have somebody trying to steal somebody else's cheese, you have to go give them something that they haven't thought about. And you want to make it very clear, when they've crossed the line, that there are going to be repercussions. So I think we will have layered international cooperation that'll allow us to be a collection of nation-states enforcing these behaviors and also be able to act as individuals in order to do the strength of the individual where it's important and the strength of the collective where it's important.

LT. GEN. HAMEL: If I might, I think that this whole topic and area is yet another example of how we've allowed ourselves to become drawn into a highly polarized and, in some cases, political and ideological debate and we've really lost sight of what the real true national interest is here. I think one of the steps of moving forward here is a discussion such as this, where you really try to be able to highlight, what is the harm that we have induced upon ourselves in unintentional consequences?

I think the other part is to also be able to come to grips with what in many cases is the futility of the path that we're on. It's not achieving the desired effect but it is causing unintended consequences.

Some of the propositions that we see today – and we heard this morning a bit about trying to raise the barriers higher on those things that truly are sensitive technologies. At the same time, we try to enter into much more productive kind of relationships, if you will. And routinized is one facet of that overall.

I would come back to something that Gen. Fogleman touched on. I think that one of the other parts – and it does relate back to my earlier point that I think we need to have a layered approach here and a more sophisticated outlook – that is, there will be places for very sophisticated capabilities and critical enabling technologies that we indeed want to be at the forefront on and protect.

But increasingly, the real value of space is how it is that we can integrate it into very practical applications, whether we're talking about civil uses or military uses. In that particular case, our interest is being able to leverage our ability to manage large systems and networks of capabilities and it's not about the eashes of the circuits and the optics, but it's rather about the technical wherewithal to be able to bring that. That's where I think a lot of the benefit is going to be in the future and one in which we can actually share with and find common ground with friends and allies.

MR. HAMRE: Ron, did you want to add something?

GEN. FOGLEMAN: I would like to just briefly pick up on a term that Jeff used, which was cyber hygiene. I hadn't seen them put together that way.

And I'm going to talk just very briefly about a program that the Air Force has now implemented in this area. And I had nothing to do with it and quite frankly, when I read about it, I was initially a little put off by the whole thing.

But the fact of the matter is, recognizing the cyber threat, the Air Force has now put into their basic training for every airman that comes in the United States Air Force a cyber awareness, cyber toolkit, if you will, training with the idea in mind that as a military force, we are engaged in many ways in combat.

But the idea is that from day one when you put on the uniform, or if you're in commercial business, whatever, you are engaged in cyber warfare. And if you don't – if you are clueless about one, that it's happening or two, how it's unfolding, you're going to be a lot more vulnerable than you ought to be.

So I think this whole idea of cyber hygiene across the various entities, whether they're business or government or military services, whatever, is the beginnings of – or, can provide a building block to get us away from this Maginot Line kind of defense that Gen. Cartwright was talking about earlier and start to think about different ways to protect ourselves in this cyber arena.

MR. HAMRE: Let me just, if I may, pick up on the comment you made, Ron, that our problem with technology control is really going to be with the Congress. I was over at DOD at the time when we were wrestling with the Congress over what was the definition of a supercomputer. So it was a 7,000 megaflops or some damn thing – I never knew what that was. I thought gigahertz was a French car rental company. (Laughter.) What the hell? I didn't know.

And then when it became obvious that the next Xbox was going to meet the threshold of a supercomputer definition, we certainly didn't have a policy framework that made any sense. So our problem is technology moves at 5x speed and policy development moves at .8x speed and political consensus around technology forms at .2x. We have such a disconnect in these speeds of consideration and how will we manage that with this Congress, any Congress? It's going to be a real challenge.

I'm going to pose one last question, if I could: When are you guys going to start doing the work here? Let me pose one last question here which is, we've had a grand debate that's gone on as long as I can remember over architecture in space. Should the economics – and technology drives this to high fidelity: very big, very expensive platforms, and of course because they are so big and they're so expensive, we have to make them last a long time and because they're big and expensive and they last a long time, we buy very few of them.

You see the spiral. We've been in that space. And yet we've had this allure of network space for a long time – probably the only thing close to today would be GPS – but the idea that there are low-cost, low-fidelity assets that in the composite represent an alternative of equal capability and potentially more survivability.

This seems to be a debate that's in front of us again that appears to be tying the department up in knots as they're trying to think about a new space policy. Jeff, I think you are in the middle of one of them. Why don't you open some thoughts and then we'll open up and then, all of you?

MR. HARRIS: There's a little bit of Garrison Keillor in it, with everybody sort of above average. I come from an organization that has probably built more small sets than any other organization, if I go back in history, and, by NRO responsibilities, some of the big, capable, long-lived collectors.

What we've now come down to is smart people, when they're doing a weekend project, open up the drawer in the toolbox and pick the right tool for the job. People who don't practice the craft think that, correctly, most anything can be used for a hammer. If the surgeon takes that same approach, I urge you to pick a different surgeon. If you're just hanging a picture on the wall, maybe you get by with only a bruised finger because that stapler is awfully attractive compared to walking down the hall to drive the nail into the wall.

So what we have noticed is that people want to subscribe to the headlines, not think about problem we're really solving. Years ago, we talked about how platforms would provide a specific capability and increasingly, the words "network" and "architecture" and "enterprise" all come together. So when I start to think about space systems in a cyber enterprise operating together, consistent with Gen. Cartwright's remark this morning, I tend to deemphasize the platform a little bit and I can take a collection of platforms in order to go cause an outcome to take place.

So if you say, why is a space platform a given size, there's lots of things that are simple things that Kepler tells us about orbits, but the rule that you want to write down and keep in your

pocket protector is the power aperture of how do you get enough gain on the signal that you are trying to collect, whether you're receiving imagery or signals. And that – although technology has helped that a bunch – alongside the football stadiums you see the guys holding big reflectors, parabolic reflectors, in order to increase the gain on the signal that they want to do.

So if you're interested in finding needles in needlestacks, the reason your cell phone batteries last longer than they did when you were carrying around the bricks is we are actually transmitting at lower rates. And when you have your four or five bars on your phone, the transmitter is actually turning down the power, which is really good for your battery but it's also good for network utilization because you can get more calls and more money coming through the system. And so the system is balancing itself as a system.

And back to your question, John, we will balance our capabilities that says, can I put the sum of the parts together as a greater whole? So if I look at what we're doing in the intelligence domain of multiple intelligence fundamentals coming together to solve a problem – a little bit of this, a little bit of that, a little bit of this – we get to an answer much quicker when we talk to all of our now-integrated cylinders of excellence.

Let me just take one more step. We keep wanting to make this a cyber and a space. If at the second I put, let's say, space into extremis, I turn to my enterprise and I ask an F-22 or F-35 that's screening into prosecute a battlefield to use some of its sensors in conjunction with the enterprise need for information, it is an eye-watering capability in order to go take that and put it together.

What else you might then add to this mix? If I just swing around to the right IP address, I get the traffic camera. So when I'm putting together true situational awareness systems, the kind of stuff that Jack Bauer uses on "24," it's not some fairy dust in some fairyland. Hollywood can take lots of advantages with physics, they actually don't take that many advantages with what you can do with information systems integration.

So as I pull all this together, I think, John, I will naturally start to right-size systems. I don't have to have the religious debate that the proliferating constellation outwins the larger single-item constellations because we tend to talk about handfuls of assets in the platform space that Gen. Cartwright told us not to speak of.

To quote one of the attackers in Ron Fogleman's wargame example, he said, fine, you triple the number of satellites, you add the capability for an extra 40 minutes or an hour. Because if the enemy is very capable at attriting your force, you better figure out a way to attrit your enemy. Thank you.

MR. HAMRE: Ron, you're an old programmer – you've got to face this issue.

GEN. FOGLEMAN: Well, as an old programmer, I believe that architectures are very useful and even vital but I think we have to think about them a little differently from time to time. Historically, if we thought about an architecture for space or delivering space capabilities,

it was pretty much a national security undertaking. I believe that because we have new players in the game that that gives us new opportunities and probably different capabilities.

And so as we go about building a space architecture today, I think we have to include the commercial sector, very definitely. And again, it seems like I'm beating this drum on the ally thing but we have to get our allies and partners engaged on it, both with space and terrestrial assets.

LT. GEN. HAMEL: Just this final thought, perhaps. Architectures are useful tools to think about how you bring together individual elements and orchestrate them in ways to achieve a whole. I think one of the things that we perennially find as we go into the kind of wargames that Gen. Fogleman was describing, that the vast majority of our experience today is informed by peacetime uses.

When you actually get into, now, focused issues, problems, challenges in a particular theater, or when a thinking adversary takes actions that now thwarts your capabilities, you have to think differently about what are the elements of an architecture?

Frankly, I think today we find ourselves where, in some of those wargames, that many of these things almost become self-deterring because of the individual value of an item in space. Perhaps it represents some unacceptable loss.

And so the whole calculus of how we think about architectures – I do believe it's not just what we buy and operate with, but it's also other elements that could come from the commercial sector, that could come from allied participation – and then how do we ensure that we can actually interoperate and have standards that will allow us to be able to actually bring those together? I think that's what the benefits of architectures are, is they force you to deliberately think through that.

MR. HAMRE: Okay, what we're going to do is I'm going to open it up here for questions and I'm going to ask you to pose it to one person and if any other colleague has a something, to jump in. That way, we're going to get more questions in. John, we'll start with you.

Q: Sorry, two questions for Jeff. The \$40 trillion – could you elaborate on that a little bit? The second: If a nuclear missile comes at America, there is a response. If under-priced tires come in America, there is a response. What thought has been given to the nature of a response to cyber attacks? What does and would America do?

MR. HARRIS: I meant to check my notes this morning – I believe I was in a conference a couple weeks ago and if I'm not mistaken, Adm. McConnell used the \$40 trillion in some remarks that he gave at a conference. We focused this morning on attribution for cyber because it is difficult – because I tend to do a much better job finding it logically than I find it physically and the people that I want to talk to tend to live in the physical domain over the logical domain. So I have to close that.

If you take a look at where we stand on prosecuting cyber crimes, I think we're doing better. The big industrial theft are credit card information. We have a couple sizeable cases to where we've traced it all the way back. I think what we have to do is turn up the speed in the game.

I think across – in asymmetric nation-state or non-nation-state warfare, I think we're having these discussions so we can work on holding people responsible for what they do. And I believe the countries of the world are tolerating behaviors on their systems and networks that we're going to have to tighten up significantly and hold people responsible. Until you do that – and I'm back to just getting the good behaviors so that – in the Wild West, we all carried guns and as we evolved the societal norms –

MR. HAMRE: Ron still is. (Laughter.)

GEN. FOGLEMAN: Out in Durango – (laughter).

MR. HARRIS: The Durango people, yeah, think it is – they read the first article differently or something. (Chuckles.) So I think it's very much work in progress, but I think we're having these conversations because just the fact that you type it on the computer doesn't give me free access to it.

Q: Thanks. I'll address this to Gen. Fogleman but both Gen. Fogleman and Gen. Hamel made remarks right towards the end about the importance of an understanding of an architecture. What I would propose right now is we have two architectures.

We have an evolving – well, we're trying to develop an understand of what a government architecture would look like. But we also have an independently-evolved commercial architecture. Some of the facts are that 75 percent of the commercial capacity is in the hands of four companies, none of which are American – the geo-orbit. Eighty percent of government traffic – and a very well known stat – is actually traveling on those satellites, not on government-owned systems.

Yet there are these two different architectures, which means you don't really have an integrated architecture at all. The question that's embedded in all this is what can we actually begin to do about that because at the moment, it represents a tremendous vulnerability. Just as a final observation, the consequence of not integrating these architectures is very, very easy to understand on the commercial side.

That is, that companies like SES, the company I work for – when I go to the board of directors and say, you want to build this capability into a spacecraft because DOD needs it? They're not interested in hearing that because I can't really take them anything that's actionable in terms of what kind of commercial opportunity that might represent.

So this lack of coordinated planning, lack of integrated architecture, lack of engagement in the early stages of developing needed capabilities results in the commercial players, upon

whom the U.S. government is very dependent, investing on behalf of their commercial customers and not the government that actually needs them to invest.

GEN. FOGLEMAN: Well, I'm going to slip back into a portion of my military career where I was the commander-in-chief of the U.S. Transportation Command, having spent most of my life doing something else and then suddenly being sent off to the big airplane business. One of the wonderful revelations that occurred as a result of that was to begin to understand the Civil Reserve Air Fleet concept. The direct applicability is probably not there but the concept is there.

Just by way of review, back in the 1950s, the Congress decided that they would pass a national transportation act which basically said that the United States military will get out of the passenger-carrying business in aviation and that the military would depend upon the commercial business to do that. The military could and would in fact be responsible for building aircraft with unique military capabilities, primarily cargo kinds of airplanes.

That led to a whole series of understandings that in the end, resulted in a coordinated, enmeshed kind of architecture on how we would go about providing strategic lift of people and things in the event of a conflict. Today, I think that fundamentally, the way this 80 percent of the capacity that's being carried on commercial satellites is bought is on the spot market, in a sense. There's no forethought; there's no sense of trying to become partners, integrated kinds of partners.

So I believe that that's the step that has to take place. As I say, I'm not sure it's got 100 percent applicability but somebody has got to raise it to the next level that says, we have to have some kind of an existing and standing relationship. Now, the whole craft thing gets complicated by foreign carriers and what we're talking about. But, as you point out, we're already buying the capability on foreign assets so we ought to, in some way, make this a deliberative planning process rather than an ad hoc, buy-on-the-spot market.

MR. HAMRE: All right. Right down here. Mike's coming on to you – yes, sir.

Q: I'll direct this to Gen. Hamel, but it really is a follow-on to Tip's question. As you look at this gap, you talk about space as a critical enabler and this growing gap between the military requirements and, let's just say, the capacity available for the military networks.

From a financial perspective, we're seeing a lot of parallels unfolding in commercial space to what has unfolded in commercial shipping, where largely, ships are a commodity; they're all produced outside the United States; they're all owned outside the United States; they're all registered and regulated outside the United States; and they're operated by nine U.S. companies. Is this the future path of commodity space capability or capacity, for lack of a better word? Does it matter?

LT. GEN. HAMEL: That is a great question. I think I maybe start with the latter points you made. I do think it matters a great deal. One of the things that, as we take a look at – Tip's question touched on and kind of illustrated that today, we do have different kinds of capabilities

between what are our governmental systems and use of spectrum, orbital slots – things that nature – versus what are commercial.

And so one of the things that really is important if we were going to be able to derive our defense and security benefits is that we have to be able to foster standards and interoperability criteria and the like that are not simply going to operate in the marketplace, if you will.

So I do think it's very important that we have an active U.S.-led effort in terms of, what are those architectures? What are those standards and the like? I don't think you can do that if you're simply going out of the commodity market, if you will, trying to buy what's available in the marketplace.

So I do think it's twofold. One is that we still enjoy technological advantage in terms of the kind of systems and products we produce in this country and to simply recede from that and abdicate it, I think, would be a real error. But the more practical part of it is, it's very difficult if one thinks about something like GPS.

One of the greatest benefits of being able to define the requirements, the standards and the like that now has – it isn't just about the satellite in its orbit as how it is that we have been able to be at the forefront of really leveraging the advantages and the applications of GPS on the world markets. I think that's the sort of thing that you end up losing if you simply abdicate that marketplace, saying, we'll just go to foreign providers.

MR. HAMRE: Ron?

GEN. FOGLEMAN: Yeah, again, going back to the shipping example and particularly as you start to look at how you formalize some kind of a relationship with the satellite manufacturers and particularly those who are foreign manufacturers, you need to remember that in the shipping business, there is this thing called the Jones Act, which basically says that if you're going to use ships in the military, they better have been built in the United States and fundamentally operate through our system – there are ways you define that.

This may be a two-edged sword, in a sense. As we start to more formalize this, there will be those elements who will try to take us to the extent that you can buy America, all that kind of stuff. So you got to watch that this isn't a two-edged sword, I think.

MR. HAMRE: Ma'am, down here, and then Tony and then I've got one from the Internet and we'll wrap up, I think.

Q: Yes. I'm Paula Gordon; I have a website called gordonhomeland.com; it does consulting and educating. I was deeply involved in Y2K and I would like to direct this to anyone who had extensive background in that. I see a possibility of capitalizing on the lessons that should have been learned and could have been learned and can be learned still from Y2K and the way we organized to do that.

I'm thinking of the proactive approach that was taken not only by GAO and the Congress but also DOD and extraordinary things that were done behind the scenes. The full story has not fully been told: the role that the White House played with their coordinating effort and also the U.N. and their Peace Corps-type technology dissemination effort throughout the world. The key here, I think, is a common sense of purpose and mission and organizing around that. And I think this could be very helpful internationally as well as domestically and I'd like to get some reaction.

MR. HAMRE: If it's okay with you, I coordinated Y2K for the Defense Department and spent a lot of time on it. Of course it had the advantage of being a defined problem, a time-defined problem. But even then, we made – Pete Kind is back there; Pete ran the thing for the administration.

We made very little progress on Y2K until Congress passed basically a waiver on anti-trust and confidentiality issues, until Congress basically said, it's okay to talk about your problem and we're not going to let anybody sue you because you talk about your problem. We made virtually no progress until that legal impediment was removed. The private sector was very resistant.

I think we have an analogous problem here. The private sector does not trust the government to share all the problems they're having in cyberspace. They are afraid if they come forward that the government's going to regulate them or word is going to leak out and they're going to get punished on the stock market because their shares are going to go down. There isn't this fabric of trust. I think this legal framework would be very important for us to try to get our arms around because I think that's the bigger lesson I learned from Y2K.

Tony Tether and then I got one from cyberspace and then we're going to wrap up.

Q: Thanks very much. The title of the session was "How to Stigmatize the Use of" and I haven't heard much of that. Now, I thought that John Hamre mentioned the problem in the right way: that this a problem that can't be solved but we manage it.

It's like somebody killing somebody. First question is, who did it? That's the attribution part. But then there are published responses for somebody who did it. If it was manslaughter, jail term; if it was second-degree murder, a longer jail term; first-degree murder, your life is taken.

But these are all published responses. What I haven't heard is – we talk about one, the attribution, but I haven't heard any ideas of, okay, what are our responses going to be, other than sending a demarche? So, for Gen. Fogleman, somebody has taken out our satellite. We know who it is. What's our published response?

GEN. FOGLEMAN: The simple answer is, we don't have a published response and my own view is – now, there may be something that I'm not aware of in some classification level – but by and large, the reason we don't have any published response to this, in my view, is that we

have not had the opportunity for the senior policy leaders to look through and develop, if you will, the codes, the standards.

That's what determines how you define a crime and we just haven't had those discussions. I don't think we've had those discussions at the right level to understand. We refer to them as rules of the road or whatever, but, Tony, I –

Q: Well, you know, we've had plenty of those discussions but we've never come to any conclusions. But until we do, we really haven't stigmatized them. That's what seems to be the issue.

GEN. FOGLEMAN: Again, I'm coming back to beat this drum that says, when the Chinese shot down the satellite, people looked at that in a lot of different ways – or destroyed the satellite – but it wasn't until people brought this debris issue to the forefront and showed that it was something that, just as a criminal code exists for the common good of society, that here was an act against the international community, that you saw this thing stigmatized in a way that I think completely surprised the Chinese as well as a lot of other people.

But you, Tony, as you always do, you're out there on a leading edge with a question that I'd like to be able to give you a satisfying, hard answer but unfortunately, I just don't think we're far enough down that line and it's a shame.

MR. HAMRE: We need a DARPA for policy. (Laughter.) I've got one question from cyberspace. We're webcasting this and I've got a very interesting question from somebody out in cyber land who said – and this is to any one of you and you'll all probably want to avoid it, okay – (laughter) – and that is, what role can offensive actions by a government take to create an eventual normalization of this lawless state in cyberspace? Anybody want to – Michael, do you want to take that on? You're the youngest guy here so you're a –

LT. GEN. HAMEL: I don't want to duck the question but I do not feel as though I can even speak intelligently on the question of cyber.

MR. HAMRE: Yeah, please.

GEN. FOGLEMAN: I just want to look at the question. (Laughter.)

MR. HAMRE: Well, I reframed it just a little bit to make it juicier.

MR. HARRIS: Fifty percent of the computers in this country don't have firewalls or antivirus software installed on them, as we sit here this morning, according to a recent article in USA Today. So when you use the word "offensive," for many groups in Washington, D.C., you think of something different.

So it's fairly straightforward for someone to cause your computer not to work because you've taken no protection for it to work. So if you live in a glass house and you don't lock your doors and you don't take any of the minimum things to stigmatize bad behavior in some way, so

I think we will raise the bar. We will get attribution and in that process, if you do something bad on your computer to something on my computer, I am a firm believer that the laws of nations and the laws of society will allow for a proportional response. And we do it today in denial of service.

GEN. FOGLEMAN: In addition to what Jeff has just said, I think that it's very useful, from time to time, and I think we have this kind of capability. As we monitor this stuff, we're not going to respond to every attack, whatever. Hopefully, somebody's codifying, classifying, determining origin, everything.

But I think it's very useful that every now and then you take a shot across the bow. You sit there and you suck up these attacks but every now and then, I think we have to institutionally – and I believe that, as we stand up a unified cyber command and we have a service component that this needs to be part of this.

It doesn't have to be a big public pronouncement that we have done this or we haven't done it. But I think that this command has got to have the kinds of authorities that allows it, from time to time, to take a shot across the bow at somebody who is being persistent or just being a nuisance, if you will.

MR. HAMRE: Ron, I think you made news. (Laughter.) Ladies and gentlemen, I think this reflects why I have so much admiration for these three gentlemen. This is a fascinating discussion we've had this morning. They've really opened up my aperture – I can't say the gain's any better, but my aperture is wider. (Laughter.) I have learned a lot from listening to them so would you please thank them, with me, for – (inaudible, applause.)

We're going to take about a 15-minute break. There will be another panel that meets in here but you may be moving to other sessions. So we're all in the same quadrant. Take a little break and come back.

(END)