



Center for a
New American
Security

THE CONTESTED COMMONS: THE FUTURE OF AMERICAN POWER IN A MULTIPOLAR WORLD

FEATURED PANLISTS:

**ADMIRAL GARY ROUGHEAD, USN
CHIEF OF NAVAL OPERATIONS, U.S. NAVY**

**GENERAL CARROL CHANDLER, USAF
VICE CHIEF OF STAFF, U.S. AIR FORCE**

**NORMAN A. AUGUSTINE
CHAIRMAN, NASA HUMAN SPACE FLIGHT COMMITTEE**

**DR. JAMES MULVENON
DIRECTOR, CENTER FOR INTELLIGENCE RESEARCH AND
ANALYSIS, DEFENSE GROUP INC.**

**ABRAHAM M. DENMARK
FELLOW, CENTER FOR A NEW AMERICAN SECURITY**

**1:30 PM – 4:00 PM
TUESDAY, JANUARY 26, 2010**

**TRANSCRIPT PROVIDED BY
DC TRANSCRIPTION – WWW.DCTMR.COM**

MR. JOHN NAGL: Ladies and gentlemen, good afternoon. Welcome to the release event for the new report on the contested global commons. I'm Dr. John Nagl and I have the honor of being the president of the Center for a New American Security.

We're honored today with the presence of four leading officials charged with thinking about and executing a strategy to manage the challenges of the contested commons: Admiral Roughhead, General Chandler, CNAS Board member Norm Augustine, a special welcome, and James Mulvenon.

Thank you all very much for agreeing to join us today. We're honored to have you here.

The great geopolitical theorist Sir Halford Mackinder once observed that democracies find it hard to think strategically in peacetime. I would argue that the last eight years demonstrate that it's hard to think strategically in wartime as well.

For the past eight years, U.S. strategic thinking and our broader foreign policy have been dominated by the wars in Iraq and Afghanistan and the broader campaign against al Qaeda. While this is certainly justified given the vital national interest at stake in all of these wars, this focus on our immediate security challenges must not come at the expense of a broader discussion of rapidly changing international dynamics.

We face a world in which attacks on our information networks and our satellite systems present real challenges to the freedom of navigation of virtual domains even as we face new threats to freedom of navigation in the air and maritime domains.

This study of the global commons takes a hard look at the commons as a critical element of the international system. It identifies American interests in the commons, challenges to those interests, and then proposes recommendations to maintain their openness and their stability. The global commons is also expected to figure prominently in the "Quadrennial Defense Review" and other national-level discussions of the threats and opportunities the United States faces in this 21st century. We hope that our report will serve as an intellectual foundation upon which future analytic efforts can build.

In addition to thanking our commentators today, we'd very much like to thank the Smith Richardson Foundation and all of our sponsors and friends for their help in making this research and this event possible. And with that, I'd like to turn things over to the report's primary editor and author, CNAS fellow Abe Denmark.

MR. ABRAHAM DENMARK: Thank you, John. I personally am very honored to share the stage with such a distinguished panel. I'd like to thank them all for joining us this afternoon. I'd also like to thank my coauthors many of whom are here today, especially James Mulvenon on the stage with me for putting together what I think is a helpful report. In addition to the capstone chapter that we have distributed today, CNAS has produced a full edited volume that includes what I think are excellent papers on all four of the global commons. This report is publicly available on the CNAS website.

I'd also like to join John in thanking Smith Richardson Foundation for their stalwart support of this project throughout the entire process. I'd finally like to extend my personal thanks to our director of studies, Dr. Kristin Lord, for her wise advice and her tireless assistance throughout the production and editing of this study.

John's remarks today rightly describe this report as part of a broader effort to reexamine the foundations of American power and the challenges that we will face in the coming years. Since the end of the Cold War, the United States has protected and sustained an interconnected international system that has enabled people, ideas and capital to freely crisscross the world with little regard for international borders and has given emergent regional powers new influence over their own destinies.

This global system is enabled by a fundamental physical openness of common spaces from transport over the seas and through the air to the use of space and global communications network, our daily lives are enabled by this openness.

This did not happen by accident. It's the result of decades of effort by governments and private corporations to build a system of systems that allows for global commerce and interaction. These systems exist within and between the global commons, the seas, air, space and cyberspace.

Today, for example, over 90 percent of global trade, worth over \$14 trillion in 2008, travels by sea. Civil air transportation carries 2.2 billion passengers annually. Governments, militaries and corporations around the world rely and space for communications, imagery and accurate positioning services. And finally, financial traders in New York City use the Internet to transfer \$4 trillion, greater than 25 percent of America's annual GDP every day.

This dominance has since World War II been protected by U.S. military dominance and sustained by American political leadership, yet this dominance is becoming increasingly contested with profound consequences for the world's access to the commons and the power of the American military.

The free flow of capital around the world is facilitating the emergence of a multipolar world giving rise to new centers of power. Some of these new powers are using their newfound wealth to acquire and develop high-end anti-access capabilities that could undermine the openness and stability of the global commons. Ironically, some states are developing capabilities and policies that threaten the very international system that has made them stable and prosperous.

Simultaneously, globalization and technological advancements have lowered the threshold for poor states and non-state actors to acquire disruptive military technologies.

These two trends will complicate an increasingly challenging and complex security environment. In addition to our ongoing commitment to deter and defend attacks on U.S. interests and our allies', Pentagon assessments suggest the United States in the coming decades will confront a greater number of threats across a broader spectrum of warfare in a more geographically diverse and challenging number of hotspots than it has in the past.

From failed and failing states to insurgencies and terrorists around the world to disasters and conflicts related to climate change and resource competition to challenges in the global commons the U.S. military is going to be busy.

Taken as a whole, the future security environment will test American leadership. Protecting open access to the global commons will be in high demand but the capacity of the U.S. military to protect the commons will be challenged by new commitments and increasing diverse set of military threats. The status quo in which the United States is the soul guarantor of the openness of the global commons and other free states free-ride is unsustainable.

Despite the emergence of an increasingly complex set of military threats, it is important to remember that it is not America's absolute power and influence that is falling, but rather its relative power compared to that of emerging states. While American dominance may be contested in the coming years, America's ability to lead remains.

Our study calls for renewed American leadership in the global commons and advocates a broad and multi-pronged strategy to preserve the openness of the global commons that recognizes the realities of the emerging multipolar world.

This strategy should be firmly founded in the best tradition of American institution building and with the recognition that the United States can no longer protect the common alone.

The United States should develop and enable an international system which in turn nurtures a loose set of international agreements that effectively preserves the openness and stability of the global commons. Additionally, the United States should adjust its military capabilities to defend and sustain the global commons, preserve its freedom of action in commons that are contested and enable effective military operations should the commons become unusable or inaccessible.

Specifically, the United States should renew its commitment to the global commons by pursuing three mutually supporting objectives, namely, building global regimes, engaging pivotal actors and reshaping American hard power to defend the global commons.

Yet these commons are all unique and America's strategies toward each must be tailored to the laws, norms, military advantages, interests and pure physics of each commons.

To provide insight into the nature of the commons, we have invited four senior leaders and experts to provide some insight and expertise on their respective areas.

I'll introduce them each individually and ask them to make formal remarks. Once completed, we'll have a short discussion amongst the panelists and then we'll have some Q&A with the audience.

Now, in our study we had to figure out an order in which to present sea, air, space and cyberspace. We chose to discuss them chronologically by which each commons

became accessible to man. It's a bit arbitrary but we had to pick some order and that's what we went with and that's what we're going to stick with today.

So first I would like to introduce the Chief of Naval Operations Admiral Gary Roughead to discuss the maritime commons. He's a 1973 graduate of the United States Naval Academy. Among his many accomplishments, Admiral Roughead was the first officer to command both classes of Aegis ships and is one of only two officers to have commanded the fleets in the Pacific and Atlantic Oceans. Other previous assignments have included commandant of the United States Naval Academy, deputy commander of the U.S. Pacific Command, commander of U.S. Pacific fleet and commander of U.S. fleet forces. Admiral Roughead awards include the Defense Distinguished Service Medal, Navy Distinguished Service Medal, Defense Superior Service Medal, Legion of Merit, Meritorious Service Medal, Navy Commendation Medal, Navy Achievement Medal and various unit and service citations.

Sir, thank you for coming.

ADM. GARY ROUGHEAD: Well, thanks, Abe. I guess my presentation is properly entitled "The Old Man and the Sea." (Laughter.) But it is good to be here with you today, and although the topic is about the contested commons, I'm somewhat of an optimist and I think that while the commons at times are contested, they also foster great cooperation.

Witness what is going on in Haiti today with international and interagency cooperation at levels that, quite frankly, are unprecedented and not unlike the tsunami of 2004 it's the commons that bring people together, the commons that allow them to operate in ways that they would not otherwise be able to operate in because of the open nature of what we deal with. We're able to park one of the world's largest hospitals in that common to take care of the suffering there and at the same time put capability in there that provides things such as food and water and fuel to take care of the crisis.

But as we all know, the commons are not always so benign. As a Navy, we are operating and reliant upon all of the commons that are discussed in the report. And we've observed first hand how the stability of these commons and the access to them is essential to American security and prosperity and also to our military operations. There is no question that we would not be the dominant naval force in the world today without capabilities in each of the commons. Denial of access in any of those domains significantly hampers our operations.

So what is at stake in each one of them?

In space, although much of the work there is done by our great Air Force, the Navy has responsibility for significant communications capabilities in space that are used by forces on land and at sea.

In cyberspace we in the Navy operate the largest corporate intranet in the world with over 700,000 users and 360,000 work stations alone. It underpins a vast array of our activities and operations.

What is at stake at sea? It is commerce, communications and power projections and resources. It was already mentioned the amount of trade that moves on the world's oceans and that trade has been going on since the beginning of time. But it also enables countries to pursue livelihoods, to draw their resources from those commons and an area that I've recently visited – for example, in Iraq, where about 95 percent of that country's GDP depends on access to the sea as it moves their oil out to market.

In the area of communications, many think and of course in Washington and particularly in the Pentagon where your life is defined by these PowerPoint images that fly around when we talk about cyberspace, it's the lighting bolts that are flying up and down from earth up into space and back down again but I will tell you that the Internet swims with the fishes because it's this transmission of information, of data, of trade, most of it runs on the bottom of the ocean. And even though we think in terms of cyberspace as its own domain, it relies heavily on being able to reside on the bottom of the ocean floor.

Resources are going to become increasingly significant in the future and we often think in terms of the mineral resources. But as we see changing conditions around the world driven by changes in climate, there will be competition for what I call the protein stocks, the fish stocks of the world will move and there will be great competition there as well. And the ability to project power also comes from the commons. As is our case with our ability to operate from our ships, our submarines and aircraft where we use the global commons as our launching point from our aircraft carriers, and as you pointed out in the report, about 75 percent of the strike sorties came from aircraft carriers at sea during the conflict in Iraq.

The stakes are high and clearly, as we have seen developments around the world, we cannot the commons for granted. Global investments in the proliferation of anti-access and area denial capabilities are visible, especially in things such as quiet Diesel submarines, advance cruise and ballistic missiles. These are investments that are not just being made by states but are also being made by non-state actors.

In preparing for dealing with these challenges, indeed confronting the challenges, we are guided by our maritime strategy that we issued just over two years ago. It was issued by myself, by the Commandant of the Marine Corps Jim Conway and by the Command of the Coast Guard Thad Allen.

And it's a strategy that focused on three things, the first being prevention where we made the statement that we considered preventing war as important as winning war, but prevention requires that there be credible combat power, requires that there be forward presence that assures our allies and deters our adversaries. It also relies on engagement and communications to prevent misunderstanding and to enhance understanding.

The second aspect is in capability where we have highlighted that our capabilities will be found in forward presence, in being a deterrent force, being able to project power, being able to exercise sea control in the maritime domain, being able to provide for maritime security and also being able to conduct humanitarian assistance and disaster response.

To enhance our capabilities, this past year I've reorganized my staff to better deal with the issues of operating in the commons and also moving the Navy in a more focused way into what I would call the new commons, particularly cyberspace. I've merged my director of intelligence and the director of communications into one entity.

We have created the 10th fleet or the cyber fleet which we will stand up at Fort Meade this Friday. And we have created what we're calling the Information Dominance Corps where we have brought together intelligence specialists, information technology specialists, meteorologists, geographers, cryptologists are all into one corps where they retain their individual identities when you bring that group together that represents 44,000 very professional sailors.

Bringing all of this together I believe will focus our efforts in a much, much more effective way. My focus also today is on capacity and even though when we look out on the commons and we can think about the ways that we can sense and influence events, it still remains that one ship can be in one place at one time. And so capacity is the greatest challenge that we face.

The other aspect of our strategy relies on partnerships because we believe there are challenges and opportunities common to many nations and many organizations. We have invested in global information sharing systems. We have sponsored the International Sea Power Symposium. It's the largest international attendance in history. This past October we assembled at our War College in Newport, Rhode Island. Excuse me – 102 countries and 91 chiefs of service. There has never been a gathering that large in the history of the world bringing all of us who have interests in the maritime domain together.

But more important than the number was the breadth and depth of the discussion – the importance that is placed on regional operations, regional constructs and ways that we can then tie the regions together in a meaningful way. So together with all of those partners, we are in essence conducting a global military operation as we bring this information together, bring the cooperation together and bring our shared view of the importance of the safety, the security and the prosperity of the maritime domain into view.

In addition to the guidance that we have put forth in our maritime strategy, I'm pleased to be working closely with the United States Air Force on the air-sea battle concept. And I'm thrilled that I'm here with Howie Chandler, also someone very familiar with the Pacific where clearly an interest in and operations in the great commons there are going to play an important role in shaping the perspective of that work that we're going to do.

We're working the project now and also finding areas for improvement such as operational integration where through robust links between air operation centers and maritime operations centers can bring together integrated architectures that we have not seen before and I think that's going to become extraordinarily important. But as we work our way through, we are both committed to breaking down those barriers for program integration because I believe when you start talking about the commons, you cannot look at it in the stovepiped way that is often the case when we deal with programmatic issues.

It's also important that we look at this as an opportunity to address the joint vulnerabilities that we may have because of some of the stovepiping that has taken place

and it also serves as a vehicle to improve the inter-service training so that we can bring the young people who serve in our military today and together in ways that we've not been able to do so in the past.

So even though there are challenges, I really do believe that there are great opportunities, opportunities to not only work together with our military with other agencies and other organizations and clearly as we have found, as we have pursued our maritime strategy for the 21st century, great opportunities to work together with nations who share the same view and who value the commons in the way that we do because at the end of the day, it will be the security and the safety that allow the commons to be the source of the prosperity that all nations in the world can enjoy.

(Applause.)

MR. DENMARK: Thank you, Admiral.

I'd like to now introduce the Vice Chief of the U.S. Air Force General Carrol Chandler to discuss the air commons. He's a 1974 graduate of the U.S. Air Force Academy with more than 3,900 flying hours in the T-38, F-15 and F-16. He's commanded a major command, a number of Air Force, two fighter wings, a supporter group and a fighter squadron. His staff assignments include tours at Headquarters Pacific Air Forces, the Pentagon, Headquarters U.S. Pacific Command, Headquarters U.S. military training mission in Saudi Arabia, and Headquarters Allied Air Forces Southern Europe. Prior to assuming his current position, he was commander of Pacific Air Forces, Air Component commander of U.S. Pacific command and executive director of the Pacific Air Combat Operations Staff at Hickam Air Force Base, Hawaii. Thank you, general.

GEN. CARROL CHANDLER: Well, first, let me say good afternoon, and John, Abe, thank you for your kind invitation. I would tell you that this is a unique and fairly timely event and as I look across the audience, it's obviously good to see some old friends and some friendly faces there and any time I can share the podium with the CNO, I know it's a great day.

But I would tell you that the Center for New American Security has taken on a strategic issue that could easily, in my opinion, be lost and overshadowed in some of the things that we're doing today in terms of conflict and humanitarian relief.

The four commons – air, sea, space and cyberspace – will play a critical and strategic role in every one of our futures. I'll give you my airman's perspective three takeaways upfront, if I may.

First, the dependable and open access to the air commons is a vital national interest and contributes to global prosperity. Secondly, increasing interdependence of the four global commons is one of the most important shifts in our international security environment. And finally, because of the second point, this requires us to reexamine the old ways in which we've done business.

Now, a noted historian, Hoffman Nickerson, wrote in 1945 that air power is a lighting bolt launched from an egg shell invisibly tethered to a base. Now, I'm thinking in fighter pilot terminology that means that if you want lighting bolts, you need secure bases.

Now, in the CNAS study of the contested commons, the authors recognized three pillars of U.S. foreign policy. First, preserving American leadership, which we've discussed briefly, projecting American power which the CNO touched on and promoting alliances and partnerships which I think we all recognize as important.

When I had an opportunity to command in the Pacific, I witnessed the impact of basing agreements in each of these areas. I also witnessed the posture of our overseas bases as threats from a variety of sources increased thus placing a premium on the need to increasing basing resiliency in this changing environment. In short, bases both enable American efforts to maintain our air commons and further national foreign policy more generally.

Bases enable control of the air as the first job of your Air Force. But air control is increasingly contested by competitors. Those with modern fighters or advanced integrated air defense systems are willing to sell them to those who have the money to buy.

Power projection in a contested air space is an integral aspect of guaranteeing access to the commons and guaranteeing international order. So given the sophistication of IEDs and threats to bases, developing a family of long-range strike capabilities is essential, in our opinion, for national security.

Just as sea control is critical to open commerce, we cannot sacrifice control of the air. The intersection of commercial and military aviation is proving critical to security as well. you don't have to go very far today to see that and our Air Force effort in Haiti along with the other services and the many institutions that were mentioned by the CNO in part provide a whole of government response like we have frankly not seen in a long time: U.S. government departments, agencies, over 30 international partners and many non-governmental organizations.

The United States Air Force's control of the air commons is enabling life sustaining aid. Within seven hours of notification, AFSOC commandoes were airborne and headed for Haiti. Shortly after landing at the airport at Port-au-Prince, combat controllers went to work and a day later there was an over 1,000 percent increase in flight arrivals from 13 slot times a day to over 145. The government of Haiti determines priorities and USAF combat controllers were providing order. C-17s and C-130s were delivering thousand of liters of water, tens of thousands of meals by air, land, and precision air delivery. At present, the AFA is controlling air traffic from a temporary control tower which we have in place and soon will be manned cooperatively with Australian air traffic controllers.

(Inaudible) – alert is another example of the nexus of military and civilian commons. Exclusively a United States Air Force mission, mostly manned by our Air National Guard, executed from 18 CONUS bases – (audio break) – confidence and security along with other aspects of security to give commercial aviation a needed boost.

Bottom line – global commerce stability and security, in our opinion, are tightly linked. A current trend such as our operations in Haiti show clearly an increasingly level of commons interdependence will be one of the most striking elements of the future national security environment. The plain fact is that neither commercial nor military aviation can operate effectively while access to logistics, as the CNO described, from the sea, whether communications and navigation from space or from information assured in cyberspace.

Unfortunately, interdependence also means vulnerability and vulnerability in one of the commons will translate into vulnerability in all. Perhaps the most challenging implication of commons interdependence is that it drives the need for greater institutional cooperation and integration. As the CNO again described, he and I live in the Pentagon on a daily basis in particular in what we describe as cylinders of excellence. But I would point out that we have a model for greater institutional integrity in the air-sea battle that again, the CNO described.

Our chief and the CNO recently agreed to pursue this strategic concept because both chiefs realize that business as usual is simply not good enough. Air-sea battle evokes the legacy of air-land battle for those of you that are familiar with the effort between the United States Army and the United States Air Force in the 1970s and '80s where the Army and the Air Force agreed to 31 initiatives to help us break down some doctrinal barriers. This has (wreak ?) benefits and continues to wreak benefits in our military in terms of the JSTARS aircraft and tactical air control parties both of which are operating effectively in Afghanistan and Iraq.

Air-sea battle in our opinion will be an enduring strategic partnership with a greater degree of cooperation and integration than we've seen in the past. And I would say that simply put it's no coincidence that the two services most directly affected by the rise of the contested commons are combining efforts at this moment in history.

So again, let me simply say that the Center for a New American Security has done the nation a great service by highlight this critical national security issue. And I hope my brief comments have added some perspective to the discussion. And again, John, let me simply thank you for having me here today and CNAS for inviting me to be with you and hopefully I'll look forward to having some questions.

(Applause.)

MR. DENMARK: Thank you, General.

To discuss the space commons, I'd like to introduce a fellow Coloradoan, Norm Augustine, currently chair of the NASA Review of United States Human Space Flight Plans Committee. There are few who are as accomplished and few who have excelled in such a diverse set of fields. I hope you'll excuse me if you let me tell you an edited version of his remarkable background.

Mr. Augustine joined Douglas Aircraft Company in 1958. Later in government, he served as assistant secretary of the Army, undersecretary of the Army and acting secretary of the Army. Mr. Augustine was elected CEO of Martin Marietta Corporation in 1997 and became chairman the following year. He served as president of Lockheed Martin

Corporation upon the formation of that company in 1995 and became CEO later that year. He retired as chairman and CEO of Lockheed Martin in August 1997.

Additionally, Mr. Augustine was chairman and principal officer of the American Red Cross for nine years, chairman of the Council of the National Academy of Engineering, president and chairman of the Association of the United States Army, chairman of the Aerospace Industries Association and chairman of the Defense Science Board.

He's a member of the advisory board to the Department of Homeland Security, was a member of the Hart-Rudman Commission on National Security and served for 16 years on the president's council of advisors on science and technology. Mr. Augustine has been presented the National Medal of Technology by the president of the United States and received the Joint Chiefs of Staff distinguished public service award. He has five times received the Department of Defense's highest civilian decoration, the Distinguished Service Medal.

He's an accomplished author, holds 23 honorary degrees and was selected by "Who's Who in America" in the Library of Congress as one of 50 great Americans. He's traveled in over 100 countries and stood on both the north and south poles of the earth. And most importantly and most impressively is a member of the board of CNAS. (Laughter.)

The floor is your, sir.

MR. NORMAN AUGUSTINE: I'm Norm Augustine. I'm an unemployed aerospace worker. (Laughter.) Space really does fit the category of resources which all of us share but which no one presumably owns and in many cases which no one is even a clear or the clear caretaker. Such commons including space are I think becoming increasingly important both as an asset as well as a source of friction.

One of the astronauts, one of the Apollo astronauts was given a T-shirt on which it had a picture of the moon on the front of it with the American flag picture sticking out from the top of it, but he said – it said "finder's keepers." Well, there is some historical precedent for that approach but it does seem that there's a better way to deal with the commons than that.

You'll recall in the early days when the U-2 flew on what's been described the edge of space. That was at the time considered by the Soviet Union to be an invasion of its domain. And on the other hand, when Sputnik overflew the United States, the Soviet Union explained that that the Sputnik had been placed in an initial orbited space and it was not their problem if the United States occasionally rotated under it. (Laughter.) All of which I think points to the complexity of the issues that we deal with here.

When it comes to the space commons times clearly have changed. Think back the competition that really drove the existence of the Apollo program and many of the space activities since then, the competition between Russia and the United States. Not many people realize but the current plan is for the next five to seven years for the only way the U.S. will have, at the end of this year, the only way they're after for five to seven years to put our astronauts and many of our fellow nations' astronauts up to the international space

station will be to buy a ticket out of Russia's launch vehicle. Times have indeed change. We have to get permission from Kazakhstan to have the astronauts launched from there.

It's a little bit like the Red Queen in Alice in Wonderland that said, why I believe six impossible things before breakfast each morning. When one looks at much of what's happening in the space commons as well as some of the other commons, particularly the cyber commons, I would think that had to be true.

Virtually all the nations do share an interest fortunately in the common use of space. The problem, of course, is that many of those nations believe they could gain leverage where they'd be the only ones to use that space. The benefits to nations are diverse – if you think of just the warning of impending hurricanes and the many thousands of lives that have been saved by that warning.

The U.S. gives away much of what it acquires in space or generates in space. Examples, of course, would be the weather data, would include GPS signals, environmental data, scientific data and so on. It's been argued that space military is the new high ground. The U.S. probably makes better use of space in that context than any other nation. That's the good news. The bad news is that the United States probably makes more use of space than any other nation and what that means, for example, is that say the detonation of an EMP weapon in space would asymmetrically harm the U.S. military capability.

Commercial firms also have an enormous interest in space and the freedom of space. Sometimes those interests are in conflict with governments, sometimes their own government. And I refer there as an example, companies that provide overhead imagery for sale in times of third and fourth-party warfare, governments may have a major interest to whom those images are sold.

And as the case with our other commons, we as citizens of this earth have already set out to pollute the commons. Today there are about 20,000 items of debris in orbit that are large enough to seriously damage a space craft. About 2,400 of them came from one event alone, the Chinese ASAT test. It's not uncommon today to have to maneuver space craft as you do ships at high sea to keep them from running into one another. And the main reason that you don't hear about collisions is they generally occur between non-active satellites given that there are only about 1,300 active satellites on orbit at any one time.

Americans tend to take this commons for granted. The best illustration I can cite to that is the situation described to you by Dan Goldin when he was administrator of NASA. He was being criticized at a town meeting for the amount of money that NASA was spending on earth satellites and the person who was criticizing him ended the argument, his argument by saying, why do we need meteorological satellites? We have the Weather Channel. (Laughter.)

As a side note to the same vane but one that's probably more important than we'd like to realize is that nothing could bring us more closely together in our interest to the space commons would be – than would be an asteroid on a collision course with earth. We don't talk a lot about that.

I checked the other day just a couple of days before I checked, an asteroid had passed within 40,000 miles of the earth. When you say that, people say that's a long way away. But think about at the scale. If the earth's diameter were the diameter of your head, you heard gunfire in the distance and a bullet went about this far from your head, you would probably be interested in that. That's why we probably should be interested in that as a subject.

Whatever the case, the space commons is of increasing importance to the military, to the commercial sphere, to the science community and to many others. There are important economic issues from a commercial standpoint. Today, a quarter of million jobs in the United States are directly dependant upon space activities and in fact there's two and a half times that many are engaged to the trickle down effect in the economy.

Unlike the other commons, perhaps fortunately for the space commons is that there are a lot fewer folks who have direct access to that commons. In fact, today there are seven countries in the technical sense that posses a full service space capability; another four who are seeking actively to reach that level, not uninterestingly including Iran and North Korea. The disaster case is a Somalia of space where we have no agreed upon rules, no enforcement and space pirates roaming freely.

And to head off such a circumstance was the goal of the Space Treaty of 1967 where we do have a treaty that's been reasonably effective. Its two principal provisions, of course, one is that space was to be viewed as used for the benefit and the interest of all humankind and secondly, that weapons of mass destruction would not be placed in space or on celestial bodies.

The issue becomes somewhat muddy because of the ability to use allied satellite systems that are based on the earth in space. Also at the time that that treaty was written, there was not the appreciation we have today of the importance of space to conventional military operations as opposed strictly to nuclear operations.

Fortunately, and unfortunately at the same time, the cost of access, the threshold of entry into space is very high which means is probably out of the reach of the – (inaudible) – terrorists, and I exclude cyberattacks from that comment.

What then might be a rational approach to the space commons, well, one view argues that nations are going to attempt to use space to an increasing degree inevitably will lead to a race and so the only way to maintain any nation's position in the commons is to participate in that race and in fact lead in it, obviously, a destabilizing argument.

A second view is that since there are so many nations that have an interest in space that benefit from it that like air and sea that there hopefully could be a general agreement not without those who withhold their agreement unfortunately, probably, but that there could be a general agreement as to the use of space that would be verifiable and that could be accomplished through political efforts.

And finally I would note that there is a firebreak in space between the positioning of nuclear weapons and conventional weapons, for example, high explosives or an unconventional conventional weapon, a high-energy laser or something like that – high-

energy beam – in space just as there is kind of a firebreak between nuclear and non-nuclear weapons on the ground.

That there's hope for such agreements I think is suggested by the existence of the international space station, 900,000 pounds on orbit today operated by many nations and with measured structure that actually works that it suggests that the possibility might be there.

I'd like to close by pointing to an error – and I hate to have to have the Center for a New American Security have to reprint all the books that they put out about this meeting, but I was certain there's a fifth space common not – space regime, not just four. The fifth one is called Antarctica and there's an interesting precedent there. About 10 years ago, I chaired for our government a commission to determine whether the U.S. should be in Antarctica anymore given the cost of being there.

And it's a very interesting policy the U.S. has. It's quite irrational, but very effective. Maybe that's the secret. As those of you who follow Antarctica would know that there are a number of nations – if my memory is right, I think it was seven at the last count – that claimed ownership of parts of Antarctica and the ownerships bounds are lines of longitude. Did I get that right, Admiral? I did. Longitude. And actually it's not that way. (Laughter.) It's this way. A pie-shaped piece is emanating from the poles and they overlap each other.

In the past, some time ago, there were serious disputes among nations over the ownership. The U.S. policy has been that nobody could own any of Antarctica but if anybody claims any part of it, attempts to take control of it, since our stations is right at the pole – we overlap everybody's claim – so we claim the whole thing. (Laughter.) And that's worked.

Today you have sharing of logistics, search and rescues, cooperative science that goes on in Antarctica, absolutely cooperative sphere which importantly is likely to work only as long as the United States or some guaranteeing nation is strong enough for the other nations to be willing to agree to such an arrangement.

Thank you very much.

(Applause.)

MR. DENMARK: Thank you, sir. I think we're going to adopt "irrational but effective" as the new CNAS motto. (Laughter.)

To discuss the cyber commons, I'd like to introduce my coauthor and co-editor, Dr. James Mulvenon. Dr. Mulvenon is vice president of Defense Group Incorporated's Intelligence Division and director of its Center for Intelligence Research and Analysis. Dr. Mulvenon is the author of numerous books and articles on the Chinese military and Chinese politics. He's also a regular contributor the China Leadership Monitor at the Hoover Foundation where he writes on Chinese national security affairs. Among his professional affiliations, Dr. Mulvenon is a member of the Council on Foreign Relations, a founding member of the Cyber Conflict Studies Association, a member of the National Committee

for U.S.-China relations and a member of the Association for Asian Studies. He received his Ph.D. in political science from UCLA and attended Fudan University in Shanghai from 1991 to 1992.

James, thank you for coming.

MR. JAMES MULVENON: Well, I'd like to thank the Center for a New American Security and my co-editor Abe Denmark. You have to admit that there's something wrong with this picture right here and it was clearly the length of my bio. But I would also just warn you to be forewarned of people who are labeled as experts, I've been studying the China cyber issue for a long time. I'm a Chinese linguist, misspent youth as a computer hacker but on one of my trips to Beijing I was scheduled to meet with the person then described as China's premier military information warfare theorist. I won't name him to embarrass him. Senior Colonel W. I'll give you the hint.

And I had sent him a message to his Hotmail account before I arrived in China. This is before the ubiquity of cell phones in China. So I arrived at my hotel, sent him an e-mail on a Sunday afternoon, told him I was there and waited and waited and waited. Finally, by Tuesday afternoon, having gone crazy watching Chinese variety shows on CCTV One, I finally picked up the phone and called one of his friends who worked at the same academy and said, why is it that – you know, I can't get a hold of Senior Colonel W. Where is he? He's always standing right here.

So I picked up the phone and I said, Senior Colonel W., I e-mailed you on Sunday afternoon and you haven't responded to my e-mail. And he says, oh, he says, well, I'm waiting for my daughter to come home from college on the weekend because I don't actually know how to check my own e-mail. In fact, I don't even know how to turn the computer on and I need her to do it for me. So that was at the time China's premier military information warfare theorist, Senior Colonel W. So at that moment, I thought to myself, you know, I need to be a little more careful about reading into the hype on so-called experts.

In the spirit of CNAS co-founder Kurt Campbell, I'd like to make four brief points. First, cyber is a commons. Second, we haven't done a terribly good job of managing the cyber commons, but we can do better. And the reason we need to do better, thirdly, is because the cyberspace commons has really changed in ways that we conduct all political and military competition. And then finally I'd like to close with some final thoughts.

It is remarkable how quickly we can accept now the idea of a cyberspace commons and in such a relatively short span of time how integral cyberspace has become to our modern life. It is interesting to point out that among the four commons, it is the only manmade commons of those and I think that has important implications that we discuss in the report for the nature of that commons itself.

But we're increasingly meshed into this dense network of the cyberspace commons. It provides the basis for ubiquitous global communications, social networking, which absorbs a tremendous amount of our – increasing large amount of our free time, enables public and private institutions to provide a wide range of services, has clearly

revolutionized the global economy in the financial system and is clearly as key enabler for military command and control logistics support.

Bottom line is the cyberspace commons is a commons that we cannot no longer live without. As my daughter, one of my youngest daughters pointed out to me in the car, when she asked me why she couldn't check her e-mail in the car. And I thought about it and I thought to myself, this is a child who has lived in a world of ubiquitous wireless broadband for as long as she's known it and it was perfectly natural to her. She says, well, why can't I check my e-mail in the car? And I think that is indicative of the world we live in.

But cyberspace is also the newest and least understood of the four commons. We certainly have had the least amount of experience dealing with issues of managing this commons. I'm a fan of the Aubrey-Maturin, Patrick O'Brian books and clearly, you know, those books are just – page after page after page of the loneliness of the sea without any sail on the horizon. We clearly have been dealing with issues in those commons for longer. Cyberspace, not so long. But we clearly know that cyberspace as a commons provides us with both advantages and challenges.

One of the advantages clearly is the speed of communications which is clear to all of us who have mistakenly hit reply all on a disparaging e-mail about one of our co-workers and as we reach into the computer to try and grab the e-mail and pull it back out. The volume of communications that we send over the Internet and all of this going on virtually unimpeded by physical barriers and political boundaries, of course, unless you live in China, Saudi Arabia and a number of other less enlightened countries.

But clearly there are major challenges in cyberspace that go well beyond the daily frustrations of applications that won't load, and constant spyware and various enticing e-mails that could improve our physical wellbeing. Our dependence in many ways has created the very vulnerability that can be exploited by a whole range of criminal and political and military adversaries.

Second point is that the United States and the international community to this point, I would argue, have had very little success in managing this global cyber commons. It's happened too quickly, too profound, the scaling has been so fast. Now, I would argue that the cyberspace commons now is largely a Wild West which should be recognizable to my most famous relative, Sheriff Billy Mulvenon of Prescott, Arizona, who broke up the notorious Grahams-Tewkesbury feud between the sheep farmers and the cattle farmers which I thought if Sheriff Billy was alive today, he'd probably make an outstanding secretary of homeland security.

But what was characterized the Wild West, little governance, users were forced to protect themselves, no one was really in charge and there was a loosely set coordinated set of protocols. The bottom line is one of the great frustrations now about cyberspace is that the least educated user who does the least about protecting their system is the weak link in a chain which can threaten the stability of the cyberspace for all of us most least of which by allowing their computer to become a – (inaudible).

Now, why is it – why is it that the cyberspace is so fraught with vulnerability and it causes so many problems? Well, the bottom line is it was never designed to have security.

The leading architects of the original ARPAnet which became the Internet would tell you that the stack of the Internet was never designed to have any security because they honestly never believed that cyberspace would have any malicious content or malicious activity. It was a just a benign environment designed to allow scientists to communicate with one another. But as cyberspace and the Internet have proliferated, clearly that lack of original design has now come back to bite us.

The second reason why we have trouble managing the cyberspace commons is because the physical infrastructure undergirding cyberspace is largely in private sector hands. So the initial impetus of any government to immediately step in and solve the problem has been thwarted or impeded by the fact that almost all of the physical infrastructure that we seek to protect is outside of government control. And thus, states do not command the cyber commons in the same way that we seek to in the sea and the air.

But all of this infrastructure exists within state boundaries and so I think that explains the tension we see between states trying to understand where the extent of their state authority lies within the cyberspace commons, either protecting the data of their citizens or defending themselves against cyber adversaries.

And thus, Greg Rattray in his cyber chapter in the CNAS report argues for viewing cyberspace as an ecological environment very similar to the sort of the global health organization view of the world in which viruses and malware are acting like diseases and that we need to have a public health model for cyber security. And I would just commend his chapter to you for those of you who are interested in that idea.

Thirdly, cyberspace has clearly changed political and military competition in the sense that weaker states are now able to compete aggressively against stronger military powers by taking advantages of the asymmetries offered by cyberspace. I personally hate the word “asymmetric” but I think it’s appropriate in this case. But these adversaries are aided by a key element of cyberspace which is the plausible deniability and anonymity that is built into both the flaws and the design of the architecture.

Now, China and Russia, I would just point out, interesting to me, view cyber as much more of an overt tool of national power, of state power. And the plausible deniability of cyberspace has given them a comfort level to be able to carry out cyberspace activity even through the use of proxies that would be unthinkable within the design of the U.S. system where we rely on people, with full-scope polygraphs who are trusted at the very highest levels with state controls. Non-state actors themselves can also facilitate the rapid orchestration of global operations across a wide area in milliseconds.

This divergence between our traditional view of cyberspace and where the boundaries are and the view of these emerging powers in these non-state actors is one of the many divergences that cyber command and other new entities will have to confront.

In closing, let me though offer a longer term view of the situation. It is easy in my view in the short term to focus on the cyber espionage issues, the recent Google-China incident, or even the medium-term issues, military and intelligence cyber scenarios. But if we really want to confront the long-term structural issues within cyberspace commons, we need to look elsewhere.

We need to look at issues related to supply chain, particularly given the global economic revolution and the globalization of information technology.

We need to look at issues related to ownership of infrastructure particularly as they relate to the CFIUS process and foreign and other adversaries trying to buy infrastructure that we rely on.

We need to look at fundamental issues of Internet governance, whether through ICANN or other organizations.

And we need to even look at the use and evolving nature of global IT standards and the extent to which decisions made now by countries like China that have a much more dedicated strategy towards enforcing a new set of global IT standards, could much farther down the line have a long-term deleterious impact upon our national cyber security.

Let me close by employing all of you to use more encryption in your daily lives, to make sure that your antivirus programs are updated, to avoid monocultures – (inaudible) – since '91 and please, please, the value of any PowerPoint briefing on China is inversely proportional to the number of censored quotes in the briefing. (Laughter.)

Thank you.

(Applause.)

MR. DENMARK: Thank you, James.

A few topics I'd like to discuss with the panel before we open up to Q&A, a few topics that were mentioned in the speeches but I think could use a little more detailed discussion. And we could just go down the table and see who wants to comment on it.

The first is something that Admiral Roughead mentioned which is the benefit of cooperation in the commons and the potential for cooperation in the commons. often we tend to look, since it's the Center for a New American Security, we tend to look at this from what can the United States do vis-à-vis these issues. but for this report and for these topics there is a tremendous amount of emphasis on working with partners, what we refer to as pivotal actors – states and other organizations that we believe can positively or negatively influence a particular commons because of their unique position, their unique capabilities vis-à-vis that commons.

So I'd like to ask all the panelists if they could comment on what Admiral Roughead talked about in terms of the potential for cooperation within their specific commons.

GEN. CHANDLER: I guess I would start with an example – and this a Pacific example. We have dealt since the end of World War II with bilateral relations in large part in the Pacific for all the reasons that you understand. In its own strange way, the tsunami and other natural disasters have brought us together in a series of relationships that have allowed us to be more multilateral in the process of doing that. And as we've done that,

we've started to see the benefit of cooperating both at sea, cooperating in the air and areas like that. So I think there're some practical applications that we see today.

ADM. ROUGHEAD: I would just amplify. I think that at least in our case, where we are working on global maritime partnerships in a way it goes back to the age nature of the maritime domain in that it has long been the tradition that you do what needs to be done, you help who needs to be helped, and then you worry about the details later. And I think that attitude prevails. But it was also interesting to see in the last four to six years how regional groupings have started to form and develop means and methods and schemes of maritime domain awareness. So I think that has been part of the air domain since its inception. And we are moving forward on that. And I was really struck, particularly this past October in Newport, how advanced some of the regional schemes have become.

I really do believe that they need to remain regional because of the drivers, the geography, the issues, the partnerships and the relationships that exist, but I do believe that they need to be connected as regional nodes, so that information can flow across those regional constructs and that's the path that we're on to do that, working with our friends and partners around the world.

MR. AUGUSTINE: On space, we have, I think, a benefit – we globally. And that is that there're, as I mentioned, not that many nations involved in space today. And so there's a chance of kind of being there on the ground floor, if you will, to build up some of these relationships, really the same relationships, I think, independent of what domain one has to be addressing or operating in. To me there are two rather fundamental ingredients of any relationship that's likely to be very effective. The first, it really does have to be more in the interest of a nation to participate than not to participate. And secondly, there needs to be some sort of enforcement for those who seek to violate the freedom, if you will, of space.

And we don't have the latter really to the extent that we do, I think, certainly at sea and probably in the air as well, but we may have to come to that one day, but unfortunately we're a long way from that because of the high threshold of entry in the space. It doesn't cost much to become a hacker. It doesn't cost all that much to attack an aircraft or to attack a ship. It's very hard to get into space and attack spacecrafts. So it's – at this point, it's hard to be anonymous. That won't always be true, but I think we have a window where we could do something.

MR. MULVENON: Well, there're some good exemplars of cooperation in the cyberspace commons already. There's been a lot of very good quiet international coordination work conducted by the State Department with likeminded countries to harmonize laws extradition, information sharing, and other things. I think there were some useful things to take away from the ad hoc coordination and cooperation that occurred during the Estonia cyber crisis with NATO and with other organizations, with other nongovernmental organizations that were mobilized to sort of beat back the assault on Estonia's cyber infrastructure.

I think nongovernmental organization like ICANN are a work in progress in this area and that ICANN in the last two years has added a significant new security element to what it's doing that has had some important payoffs and needs to be encouraged.

So I think that there're some – there're some really sort of promising examples, but I think there're also some serious impediments if we want to fully multilateralize and internationalize this at the government level, at the U.N. level, given the fact that so much of the infrastructure is in private sector's hands.

MR. DENMARK: Thank you. Another issue – a similar issue that was touched upon in the discussions here, but wasn't really fully flashed out was diplomacy and international agreements in the global commons, potential natural bias, based on the people that we have up here. I was wondering if you all could talk about what needs to happen in the future in terms of securing, protecting the openness of the global commons, in terms of what kind of international agreements do you think the United States could or should support, promote within your respective commons.

For example – not to put you on the spot, sir – our first recommendation and our summary of recommendations at the end of our report, also short one, as it's actually just two words, which is ratify UNCLOS, the U.N. Convention on the Law of the Sea. From our approach, we see international agreements as an important element of promoting and sustaining the openness and stability of the global commons. So I was wondering if you all could discuss the importance of international agreements on what needs to happen going forward.

GEN. CHANDLER: I think as the CNAS report mentioned, we've been very fortunate since the end of World War II with the ICAO, the International Aeronautics Organization that has helped nit the nations together in the way – in terms of the way we actually perform aerospace business around the world and how we deal with each other. Likewise, from a commercial perspective, the IATA has built a foundation that I think is a solid foundation. I think it's one we need to continue to build on. But as Mr. Augustine pointed out, it has to be in people's benefits to want to participate.

The goodness in this is that we've had a fairly good demonstration and the report points this out, I think, fairly dramatically. And if you're willing to participate and willing to follow the rules and willing to run an airline or a commercial aviation institution in accordance with the rules of safety and governance that are laid out, not only the organizations typically do fairly well, but the benefits that are accrued from that are also going to –will come along with it.

So I would say that if we can just continue to work the ICAO issues, the IATA issues in a governance that is in everyone's interest to be a part of, I think that not only will benefit those involved, but I think it would benefit all of us.

ADM. ROUGHHEAD: I think even though you put your recommendation first, it should have been farther forward in the book. I think it's interesting to note that my predecessors, the Commandant of the Coast Guard, myself, have long and routinely and very forcefully advocated for ratification. I really do believe that is in our best interests internationally to be party to it. And I'm hopeful that we'll see some progress in that regard.

MR. AUGUSTINE: On space, we have a fledgling agreement and it does a pretty good job of addressing issues with celestial bodies, partly because there has not been

occasion to have dispute over them. On the other hand, the Earth becomes much more complex. And one reason is that is very difficult to distinguish between a ballistic missile defense system, of which many countries are interested, and an anti-ballistic missile system in which – excuse me – an anti-satellite system and a ballistic missile defense system – difficult to distinguish between the two. And that makes writing treaties or agreements very complex.

So my fear is that the only thing that may drive us to that is some sort of a catastrophe. I hope I'm wrong and I'm thinking out loud here, but coming to the point that people lacked in their own best interest, if there's enough of a penalty for not playing ball, then people are more likely to play ball. For example, purely hypothetical, supposing you could encrypt the GPS that goes over a given – those that go over a given country, so that one country was denied GPS or other source of information, then it might be in their interest to join with others. So there probably needs to be some penalty for not participating too.

MR. MULVENON: Well, I think on the international treaty side, we have to distinguish between cyber crime treaties, which I think are growing in strength and have had a lot of positive effect, and a lot of the loose talk about international cyber warfare treaties, governing military conflicts.

The problem, as I see it, and where the cyberspace commons doesn't afford us some of the same possibilities we saw with other treaties, is that treaties have to have enforceable verification regimes in order to be effective. The problem is the very cyberspace architecture itself allows anonymity and plausible deniability that impede verification.

By contrast, the Comprehensive Test Ban Treaty employs a global network of seismographic sensors. It's very difficult to get away with a nuclear test unless it's a blow of a couple of hundred tons because there are academic institutions and government institutions all around the world that would detect the test. No similar capability exists in cyberspace and unfortunately until the architecture is modernized with better security, it would simply be impossible to enforce.

Undergirding that problem, however, or the fact that even some of the core strategic elements of cyber warfare, we're still in a very embryonic stage of even understanding that. I gave the best 10 years of my youth to the world famous RAND Corporation – you're – (inaudible) – from the beginning and Tom Schelling and Herman Kahn and Danny Ellsberg and those guys. And when you read through those materials and you try and apply them to cyberspace, you immediately run into a major problem. And it centers on this attribution issue of attacker. If you can't attribute, you can't deter.

It's very difficult to have declaratory policies if you can't attribute. And the uncertainty of effects that we see in cyberspace undermines concepts of proportional response, disproportional response. So the very strategic pillars, the foundations that we thought we had developed during the Cold War don't immediately give us the same payoff in cyber warfare. And I think we just have a lot of very hard strategic thinking to do.

MR. DENMARK: Thank you.

I have time for one more question, before we open it up to Q&A. I'd like to ask everyone to look ahead 10 or 20 years and just discuss for a bit what developments were the most and what do you think is the greatest potential opportunity for benefit in your specific – in the coming couple of decades.

GEN. CHANDLER: Let me start with the benefit and I think I would start with unmanned aerial systems. Remotely piloted kinds of systems offer us some tremendous opportunities and that goes to commercial aviation, as well as military aviation. The system that we're flying today in terms of Reaper and Predator, in my opinion, are literally the right fliers of what we're doing in the remotely piloted aircraft business. These systems will accelerate capabilities in ways that we probably don't understand completely right now.

On the other side of that coin, I would tell you that the ability of an adversary to proficiently use those types of systems can present some problems militarily. And I'm not sure it's one that we have completely thought our way through as we have looked at how they have been used in other parts of the world in conflict. And it's something that we're going to need to spend some time on.

ADM. ROUGHEAD: I'll move over to cyber, even though I'm supposed to be in the water here. But I would say the thing that worries me the most and maybe "worry" is not the right term to put on it, but that as we go forward and address what is truly an exciting new domain and dimension is that the solutions that we come up with will be based on structures and protocols of the past. And in the way that we approach our operations, in the way that we try to protect it, in the way that we try to develop the human capital that truly understands how to use it, we'll fall back at old models which are truly unsustainable, at least in the military context because we just cannot sustain that type of commanding model.

What excites me the most is cyber because I think the potential there is absolutely endless. And we have had recently – some of you may have seen some good discussions within the department on social networking for example. And there are different camps in that, but I look back on a time, a few years ago, not in that distant future or past rather, where the first time some of us heard the word "chat." It was kind of interesting. But if you look at how we command and control forces and how we move information around today, it's all about chat. When we first heard that word, none of us I would submit, maybe except for Jim here, envisioned the future that that would be how we would command and control military forces. It was just this thing that somebody had come up with. I and really do believe that in many of the applications and many of the things that we have going on in cyber today is the future, a very, very bright and even explosive future of those applications in ways that we haven't even imagined yet. And that's what I find exciting about it.

MR. AUGUSTINE: For the space, I tend to be relatively optimistic. I think that the big breakthrough will be nations cooperating to explore space, human exploration in particular. We have a good start of that today. And I see that as an opportunity to bring a lot of nations together responsibly. If I can go maybe a little bit beyond a decade or two, I think the thing that will change the aerospace entirely will be the advent of a true space tourism to hotels on low earth orbit. And if I had more time, I'd argue why I think that's not nonsense.

I think the downside, the danger is that a conflict here on Earth could spill over into space because space assets were having a major impact on the outcome of the conflict here on Earth to the point that the parties down here on Earth could not stand by and tolerate development of space assets. And that means someone will likely take out somebody's important space asset or assets forcefully. In the case of space, as I said before, although it's not thinkable at all, it's very difficult to avoid the attribution, at least in the foreseeable future and particularly during a combat period. And that has important implications. In that regard, I always think of Gene Fubini, who many of you remember as something of a legend in the defense arena. Gene told the Defense Science Board once that there is no evidence of an enemy ever successfully using camouflage against us. (Laughter.) Think about that.

MR. MULVENON: Well, when I think – I'm Irish and therefore a pessimist. And I'll resist my natural urge to talk about some sort of apocalyptic dystopia in cyberspace, but certainly a much deeper mesh – ubiquitous networking. If you just extend – even if you just extend linearly the trends now and a greater breakdown between what is commonly known as meat space or wherever we are now and cyberspace, such that the proliferation of things like virtual worlds really break down the barriers and boundaries between what we know as the reality world versus the world we then live in in parallel in cyberspace. In order for that world, though, to not be anarchic, to not be a dystopia, we need to have a fundamental revolution in authentication and in identity. It's simply unsustainable right now the way we have designed authentication and identity because with that goes privacy, with that goes our ability to maintain security. And so I think that that's – when I look and think about the things where I'm looking for the real revolutions, it's as all of this mesh increases, how are we improving authentication? How are we improving identity and therefore privacy and security?

MR. DENMARK: Thank you all very much.

I'd like to open up to Q&A. Our brilliant and stalwart interns will be walking around with microphones. I'd ask that before you begin your question, if you identify yourself and your organization.

Sir?

Q: My name is Bryan McGrath; I'm from Delex Systems, Inc. Dr. Mulvenon, given that a panel of this kind 40 years ago would not have had a chair for you and that today \$4 trillion worth of commerce moves on cyberspace every day, exactly how would government ownership of infrastructure make things better today than they are?

MR. MULVENON: Well, I think that – I don't think it would make things better. I think it would stifle innovation, but I don't want to lay my personal values on the situation. There are countries in this world in which the government does own the infrastructure and they've nonetheless been able to protect it and to succeed. But my point would be that my personal experience has been that the true driving innovation on the cyberspace side is outside of the government's sphere. And it's therefore incumbent upon the government and the private sector to actually collaborate and cooperate on protecting cyberspace.

I think it's a false dichotomy to say that the situation has reached a point where the government has to step in. My fear, however, as we discussed it in our lunch meeting is that that will be the very reaction of the government in a Pearl Harbor type scenario as we've seen from many historical examples in the past. And so it's therefore incumbent upon us to address these issues now so that we don't have that overcorrection at the point at which we have a real disaster.

MR. DENMARK: Sir?

Q: I'm Gerald Epstein with the Center for Science, Technology, and Security Policy at the American Association for the Advancement of Science. Thank you very much.

Dr. Mulvenon, if I'm not – it may be inviting you to go into your dystopia, but it seems that it was a very important point when you contrasted the differences between the manmade comments and the other ones, which really gets in a fundamental into governance. It's not like all nations on the Earth can decide to change density of water by two and all the existing ships are going to sink, but we do have the ability, if you want to go from a basically anonymous environment to one with basic authentication, that's a major change in the infrastructure that somehow would have to have a process to get there, or a path on which some people get there and some people don't. Can you see a government process that could get a hold to the basic fundamentals of the cyber infrastructure and make fundamental changes like that, which are actually in our power?

MR. MULVENON: Right, I think frankly speaking as a person who uses e-commerce in his daily life, I think there's a growing frustration by the customer base about the lack of security in cyberspace. And I think that there will be a market, frankly, for companies in that shakeout that offer better security and better options for us to continue to explore this world as it grows. And I don't think that something has to be out – imposed from the outside by policy.

I can think of at least one other very good market based solution to one of our huge problems that Packet Clearing House has suggested, which is that all of the major backbone providers in the world see all the malicious packets going across their network. If they were to come together in a consortia and say that every network, every backbone provider was – at the tier one level was simply responsible for every hostile packet that came out of their network. And that if they did not stop the hostile packets coming out their network from botnets, they'd be dropped in the peering relationships, so they could no longer guarantee their customers the bandwidth they contractually promised them. You would find them either fixing the mistake or going out of business. And the market would solve the problem. And that's a wizard solution that says we don't want the government to get involved in this, but it's also a market based solution that would virtually over night, in my view, get rid of a lot of the botnet activity and a lot of the malware activity that we see on the network.

There are also commercial impetuses, frankly, to go to the next generation internet. One of my great frustrations is that IPv6, the next generation of internet, which has much better security protocols built into it, is not a national funding priority right now. Obama has talked about it. I think we're getting there. But the Chinese and other parties are much

farther ahead on IPv6 deployment. And I think that we can move beyond this network. This network is not something we're stuck with. We can evolve it. And my point is that Betamax doesn't have to be beat by VHS in this case. We could actually – the network could actually, through market mechanisms evolve to one that's more secure.

Q: Hi, I'm Paul Bollinger with SAIC. I used to share an office down the hallway from General Chandler, so we run into each other all the time. But I think one of the greatest things I've been able to take away from this meeting is how enthusiastic Norm Augustine is. I really take that as a very positive, now, particularly someone with children that the future is a lot brighter than it sometimes can be made out to be.

I want to take a different tact on the first question that was asked, though, and say, while this isn't a decision that gets made by our military leadership, at one point, with cyber attacks going after commerce and infrastructure, will this attack merit military response? (Laughter.)

MR. DENMARK: I think you see the answer there. (Laughter.) I thought Secretary Clinton's statement a few days ago was very interesting in that it reflected NATO treaty language in terms of an attack on one is an attack on us all. Whether there's actual policy behind that in terms of what is an actual response, how does deterrence work, how do those issues work, as James very well said, I think – I don't think it's there yet. I think that's the question that's being worked in right now. Obviously if there is a catastrophic physical event that happens as a result of those things, then the theory would go away and we'd have to actually figure out what we're going to do. And the attribution there becomes an issue.

In our report, in Greg Rattray's chapter on cyber warfare, he talks about an incident a few years ago in which Chinese protesters at the American embassy were throwing rocks at the embassy in protest of – I forget what the specific event was – and argued that the government didn't have to – the U.S. government didn't have to figure out the exact trajectories of each rock, to figure out who they were coming from. They knew where they were. They know where the rocks were coming from and they knew what the message was that was being sent. I don't know if that would always – if that line of reasoning would always be applicable in all cases in terms of cyber warfare, but we need to be sure to – (inaudible) – we need to be sure to not be overly legalistic about attribution. And when there's an effect and when there's a political dimension that points to a specific perpetrator, I think that has a lot to say for beyond the specific legalisms. That's I think as much as we can say in terms of specificity.

ADM. ROUGHHEAD: And I would say with regard to the question that was focused on the military. That's not a decision for the military to make. The resources of the nation will be brought to bear by the commander in chief and I see that's how we play out, not a military decision.

MR. MULVENON: I mean that frankly we all could write the declaratory policy right now. And I fully support actually having an over declaratory policy. The United States reserves a time and a manner of its own choosing to respond to a strategic level cyber attack against the United States with the full measure of U.S. national power. What's interesting to me is internally, when these are being gamed is almost always we don't

respond with cyber because we respond in another area of national power, where we have escalation dominance. We certainly don't have escalation dominance in cyber. In almost all cases, we have a lot more to lose than the adversary does in the cyber realm.

We have a lot of other tools in national power to use at our disposal. But it does come down to this attribution issue. And Jay Healey and Gregg Rattray and the people who're working on this chapter I think rightly are trying to turn the Titanic a little bit away from this faddish about attribution of the actual attacker to responsibility for the attack, which encompasses a much wider range of things related to who could have known? Who benefits? Which government is – which government or governments is allowing this behavior to emanate from within their territory, either knowingly or turning a blind eye to it, and focusing instead on that issue of responsibility. And I think that that would actually be a much more nuanced way to deal with – because on the technical side, attribution, in my view, the attacker always is going to have the advantage, always have more ability to hide themselves. And I'm worried that it's just an infinitely recursive problem to try and figure out exactly who, which IP address is owned by which person doing what. Better more broadly to ask ourselves who is responsible for the activity.

MR. DENMARK: I also have been remiss to not cite the excellent New York Times article published this morning about the government's challenges in developing cyber deterrent policy ran by Thom Shanker among others. And I will not point him out in this crowd to avoid – so that he doesn't get mobbed with questions afterwards.

Any other – Sir?

Q: Hello, I'm Kevin Baron from Stars and Stripes. Earlier last year, out in Korea I met with the new PACOM commander, Admiral Willard, who said on his first speech on the job that the last 15 years of intelligence estimates on China's rate of military buildup are wrong. And I wonder if you have any other – if you have better assurances about the rate of China's intelligence buildup on using cyber in its military realm than there has been on China's military hardware.

MR. MULVENON: Are you going to be there in the room with me, during the polygraph helping me? (Laughter.) Yes, a lot of senior U.S. officials have come out and talked about the intrusion set and our analysis of the China origin intrusion set. There's never going to be certainty in that world, but I think – I feel entirely comfortable saying that the Chinese government and its affiliated actors are very comfortable with the use of cyber as an over tool of national power, particularly on the espionage side, largely because of what's available.

In the early days we made it too easy for them and then we have all the architectural problems now that prevent us from creating effective cyber defenses. So if I was a relatively weaker state confronting an adversary with large amounts of very valuable science and technology information or other intelligence information that was residing on the network, I would think that this was a good world to live in.

MR. AUGUSTINE: I might just add a footnote to that, that of the nine top leaders in China, these are engineers. The top nine leaders in the U.S., well we won't go there. (Laughter.)

MR. DENMARK: Yes, sir, in the back.

Q: Ben Baseley-Walker from the Secure World Foundation.

Mr. Augustine, you mentioned the questions of verifiability when you talked about potential international regulation. Whilst the ground to air or ground to space, ASAT test might be quite a test or attack – won't be quite easy to verify or easier to verify. As we move in the questions of cyber warfare being spread into the space sector, jamming frequency interference, do you really see verifiability as being such a keystone to international efforts, and therefore ideas such as an international space code of conduct, as we see these more diversified non-attributable attacks to our systems being a good way to go? Or do you see it being regulated more on a case-by-case basis, as we see new emerging threats developing?

MR. AUGUSTINE: That's a good question. I would say that I thought that attribution was of great importance in the space sphere. I think it is in all the spheres. I also said that in space it's although not at all impossible – and I set aside the cyber attacks in space – not at all impossible to maintain attribution or non-attribution in an attack, it's very difficult. And I think my answer is that I would believe that it's very important. I think it has to be somehow dealt with it in any agreement. If you don't have that, you really don't have an agreement. You don't know who you're agreeing with. And you don't know how to respond. So I think it is a fundamental.

Q: That implies that you do what I tell you to do. John Nagl from CNAS.

Norm, you talked a little bit about the Chinese ASAT test, which it sounded like – I'm not an engineer, a great disappointment of my father who was – it sounded like the Chinese ASAT action actually created 10 percent of the debris in the Earth orbit, something like 2,400 of the pieces of debris up there of the 20,000 that are there.

What was the national or American and then international reaction to that? That strikes me as an act that's not just overgrazing in the commons, but is really putting landmines in the commons. And how did the system react to that and are there lessons we can learn from that reaction, lack of reaction?

MR. AUGUSTINE: I'm not sure – I think General and Admiral are probably better able to answer that question than I, but from my perspective, as a civilian, I thought the reaction was rather mild. It was along the lines of please don't do that again. And I think the Chinese are obviously very intelligent people. They didn't do that without realizing what the consequences might be. And I think they thought that through. We're happy to live with those consequences. And they are serious because for what they – the vehicle was designed to produce fragments. It was a lot of design to do. So I think there's no surprise about and I suspect they'd probably do it again today if they had the decision to make over.

I don't mean to –

ADM. ROUGHHEAD: I think I would agree. That reaction also struck me as quite mild, but I think it was also based on the fact of the public's understanding of the domain

and what it really meant to have that many pieces up there. I really do believe that part of what must take place in the future, as people understand the seas and the air, they need to understand the impact of actions that take place in space and in cyberspace. And there is just a – not a great appreciation. I'm not being critical. I just think that that's where we are. And the depth of interest and understanding is not there.

MR. MULVENON: I don't disagree with anything that's been said, I would just point that People's Daily quoted General – (inaudible) – who is the equivalent of the vice chairman of their Joint Chiefs in a meeting with Admiral Keating, then PACOM commander, saying that he didn't not believe that there were space debris four months after the January '07 test.

GEN. CHANDLER: But you could also contrast that with the following shoot down, using Navy shooters and Air Force radars of another errant satellite that we were able to take out of orbit with no space debris. So there's a degree of technical capability, I would submit there.

MR. DENMARK: There're also – my only comment on all this is that the Americans' shoot down of the wayward satellite and the Chinese ASAT test in 2007 are actually two very different things. The Chinese action was a test of a system that didn't have to take place against a satellite that though defunct was still up in orbit and wasn't really going anywhere. Whereas the American shoot down of the satellite was against a satellite that was coming down, that was out of control and was done in a responsible way and in accordance with international agreements. Other questions? Okay.

With that, I'd very much like to thank my fellow panelists, Admiral Roughead, General Chandler, Norm Augustine, and James Mulvenon. If you all could thank them as well.

(Applause.)

(END)