SACEUR ADDRESS TO ARMED FORCES COMMUNICATIONS AND ELECTRONICS ASSOCIATION SAN DIEGO, 2 FEBRUARY 2010

Good afternoon. I do have to check my watch because I'm typically in so many different time zones in a given week: I was just down the coast in Monterey yesterday, and before that Washington; I depart here with a quick stop in Belgium and then to Istanbul for the NATO Defense Ministerial, then to Munich for a security conference, and then I honestly don't know what I do next week, but I'm sure it will involve more time zones.

I could talk about any number of topics but when I looked at the essence of what you are all discussing, I thought I would talk today about cyber space.

What I'll do today is try and convince you that the world of cyber is actually much greater than cyber war. I really want to talk about cyber space, the cyber sea, if you will, and try and kind of broaden our discussion as we think about what's crucial in this emerging venue.

Let me start by bracketing my own life in the cyber world. I started out as I graduated from Annapolis with that device on the left-hand side of your screen. Some of you may recognize it; many of you are too young to recognize it. That came out in about 1976/1977. It's obviously the Tandy Radio Shack 4K RAM on that bad boy Over there boy. on the right side of the screen is what Stephen Jobs introduced a couple of days ago. That's the new Apple iPAD. The difference in those two machines is instructive. For starters, the Tandy on the left sold for, in today's dollars, about $4,000. An iPAD will sell for about $499. The Tandy had 4,000 in its RAM. The iPAD has one million kilobytes. The iPAD is 500 times faster and the iPAD has graphics that we would recognize from the film Avatar, as opposed to basically typewritten letters on a black and white screen. This is the way the world has evolved in this cyber sea.

But more importantly than those technological advancements – and just a moment ago we heard a word about the difference between the importance of technology but the criticality of human capital – what has also changed fundamentally is what's represented by this image, which is that all of us today expect complete interactiveness.

One of my colleagues, a young officer, has a three-year-old daughter and I was visiting with him in the evening the other day. They had a movie playing on the TV and she started scurrying around, looking around the TV, looking behind the couch, and running all around getting very agitated. And her dad asked her: *Honey, what are you looking for; sit down and watch the movie*. And she said: *I*

*want the mouse because I want to change the ending.** (Note: this story adapted from original content by Clay Shirky.)

That's the cultural shift that has occurred for all of us over the same period of time that that Radio Shack dinosaur goes to the iPAD. We all expect the mouse. We all expect to be able to connect into the Internet. In 1984 there were 1,000 devices that connected to a rudimentary Internet. By 1992 there were a million devices connecting to the Internet. Today there are one billion devices around the world that connect to the Internet. And that is the second thing that links us together. First is that flow of technology, the second is our cultural expectation – we demand the mouse; we demand to be able to interact with media in this cyber sea, in this cyber space.

Also the world of cyber is becoming fundamental to education. So in addition to the technology and the cultural expectation, we see increasingly that our youngest children are growing up in a world just like my friend's daughter, demanding the mouse. This of course is the One Laptop per Child. If you're not familiar with this, I highly recommend you Google it, learn a little bit about it. It was invented by a guy named Nicholas Negroponte at MIT laboratories. It is very low-cost, extremely ruggedized, can be powered by hand-crank or solar. It is a device that flips on and automatically goes up on the cell phone architecture and connects to the Internet, and automatically connects to any other laptop, any other One Laptop per Child. So you can drop 10,000 of these in a remote village anywhere. As long as it has cell phone, it will connect the children to the Internet and most importantly, it will connect the children to each other. There are a couple of these on display at the STAR-TIDE booth out here. It is but one example of this extraordinary movement in education that is seeking to link us together. We talk a lot about strategic communications. I'm an advocate for strategic connections. That's the theme I'd like to pull through my talk today. And these kinds of devices – inexpensive, ruggedized, distributable – present us with the opportunity to connect in a very strategic and important way.

Paper money: kiss it goodbye. In ten years, this is going to phase out and we're going to see electronic transaction and banking take over. And this will further connect us in ways that we have not begun to assimilate into our cultural norms and our societies yet. As the saying goes, follow the money. As we see that shift occur – and I'll give you a practical example from my current existence, which is as the NATO Commander. I mentioned earlier going to Afghanistan. Afghanistan is going to skip the brick and mortar stage of banking. Afghanistan is going to go from paper money directly to cell phone transactions, electronic deposits. We are now paying the Afghan National Security Forces electronically, directly to their cell phones. It reduces the opportunity for corruption; it takes out a whole layer of paper distributed money; and it allows them to use the electronic medium

around their entire country, again using cell phone technology. Not what we'd think of in Afghanistan. They're on the cutting edge in this. So as I look at technology, I look at culture, I look at education, I look at where finances are going, I look most obviously at the militaries and all of these exhibitors that are linking together the security side of this, it is very clear to me that in this cyber sea, in this cyber world, we are moving as a society dramatically in this direction. Overall, that's a good thing.

But now I'd like to talk about some of the challenges that I see and how they pertain to us, and then talk about some ideas and about how all of you are part of helping us make this transition as we begin to understand this cyber world that we are sailing into very dramatically and very rapidly today.

Let me start with two examples.

These are the flags of Estonia, Latvia and Lithuania, and then the one with the crosses is the flag of Georgia. In 2007 and 2008 those four countries experienced dramatic cyber intrusions. In the first case, in April of 2007, the three Baltic republics – Estonia, Latvia and Lithuania – had a whole series of intrusions, particularly focused in Estonia, that went after their financial systems. It illustrated immediately one problem in understanding this cyber world, which is attributing these attacks – very, very difficult, for all the obvious technical reasons. The following year, 2008, the Republic of Georgia experienced not only kinetic attack but also, essentially simultaneously, electronic attack, cyber attack I should say – for the first time coupling a kinetic and a cyber attack. So this is very much a part of the security side of the dimension. I believe we're going to see more of this, and we need to understand and define what constitutes an attack in the cyber world. I'll come back to that in a few minutes.

There is also a great deal of controversy at the moment about this intersection of national entity and private/public, best illustrated at the moment by an ongoing conflictual discussion between China and Google. We don't have time to walk through the puts and takes of this. It's a fascinating dialogue and very illustrative of the intersection of private and public in this cyber world which is a very complex legal scene. So in addition to states, nations, that can be attacked in the cyber world, there is also this conflictual scene between the private and the public sector. But let me show you what really worries me in cyber space today.

It is terrorist use of this media. This is increasing dramatically and rapidly. It's hard to track it with precise numbers, but I'll give you one. Over the last ten years we have seen a 1,000 times increase in the number of websites that are devoted to what we in the West would consider Jihadist, terrorist sites. These are Hamas

guerrillas in the Gaza Strip, and you see three of them on their laptops engaged in cyber conflict. This is one aspect of it.

But even more dramatic, in my view, is the use of the Internet for recruiting, proselytizing, fund raising, attack planning, execution signals – we see all of this. So as we sail into this cyber world, we need to be aware of threats to nations, we need to be aware of the potential for conflicts between private and public but legitimate entities, and we must in my view be particularly concerned about terrorist use of this domain.

I'll give you an example of it. We read in December of 2009 in the Wall Street Journal a very interesting article about the capture of predator feeds that were taken using Skygrabber, which is a $29 programme available on the Internet that permitted, according to the article, the ability to see what our unblinking eye was looking at. So there is very real potential for insertion into systems at every level. And that particular instance could come out of any of the three illustrations I gave you a moment ago.

There is also tension in the world of cyber between the desire for openness and the very legitimate policy concerns to protect our networks. And all of us in the uniformed services today are wrestling with this. In other words, we want to be on Facebook, we want to be on Twitter. On the other hand, we want to protect our networks. So finding that balance, dialling it in, is critically important. There is nobody smarter in all of this, in my opinion, than your speaker this morning, General Cartwright – Hoss Cartwright, former commander of U.S. Strategic Command, brilliant officer, deeply embedded in all this. He said, *we cannot allow the chain of command to break the chain of information*. I think what he means is we have to find that balance and get it right. Our Deputy Secretary of Defense, Bill Lind, another extraordinarily deep thinker in all of this, recently commented, *we cannot hide behind the Maginot line of network security; we must maneuver*. And I think that is correct also. So we've got to find the right balance, and this would be the first thing that I would mention to so many of you who are engaged on the industry side of this. You need to help us with this. You need to help us find the balance by providing the technologies that will permit us to dial it in so that we can do the open strategic connecting we need to, but still protect our systems. I'll give you a practical example of a system that is doing that in a few moments.

Let me give you a more prosaic example of trouble in the waters of cyber space. This is the Facebook page of my daughter Julia. She's 18 years old and I'm very proud of her, like we all are of our children. She's a midshipman at the University of Texas in the NROTC programme. About six weeks ago, using information available on Facebook about me and about Julia, her name and her likeness were used in a complex scam to try and gain funding in a yoga Pilates programme, of all

things. This is a step back from identity theft, which is of course very extant, but it is an example of how do we protect, how do we create safeguards that ensure when we are legitimately doing our strategic connecting we don't fall prey to schemes and scams along this line. So another example of a part of this cyber sea where we need to be very careful as we sail.

And let me tell you, folks, when you take all that I've just discussed and you put it into the international venue, it becomes exponentially more complicated. Because every nation has its own sovereignty, its own law enforcement, its own approach to privacy, its own system and mores and its own networks, its own technologies. This is the table at NATO around which 28 nations sit and where I am working very hard to encourage the Alliance, in my role as the Supreme Allied Commander, to grapple with these hard issues of cyber. And again, it's not a multiplicative function. In other words it's not 28 times more complicated. It is a factor, 28. It's to the 28th power of complexity when you move this entire dialogue into the international realm. So another aspect of the challenge.

The Roman numeral V. I put it up there in the context of cyber in the NATO Alliance to make the following point. Article five of the NATO treaty is the heart of the treaty. It says that an attack on one shall be considered an attack on all. Article six of the treaty goes on to define what an attack is. It talks about geography and it talks about an attack on territory, an attack on ships, an attack on aircraft, an attack on troop formations. But guess what: in 1949 when the treaty was written, no one could have conceived this cyber world. As a result, in NATO in particular, in my view, we need to talk about what defines an attack in a country like Estonia, Latvia or Lithuania – all NATO members. What defines an attack? Because in this unsettled sea in which we sail, I believe it is more likely that an attack will come not off the bomb rack of an aircraft but as electrons moving down a fiber optic cable. So this is a very real and germane part of this challenge that we face in the cyber world.

What you ought to be saying at this point is: OK, Jim, you've convinced me that this world is linked together by all the technology and the culture and the economics and the military. We are all linked together in this cyber world. And you've shown me that there are challenges in it that range from the potential for attacks on states to that seam of private and public, to identity theft, to counterfeiting, the scams, all of those challenges. I get it. So the question becomes, what do we do about it? What are we doing about it? Let me now talk for just a few minutes about some ideas, because I think in this cyber world we are , y going to have to address our problems not by launching Tomahawk missiles but by launching ideas and technologies. And again this is where, as I conclude, I

will talk about what you can do as you represent industry and your part of this security in this cyber equation that we all face.

Fiber optic, the technology. Today again that interconnection that holds us together globally.

I like to read. I begin with literature. I begin with reading to understand. These are some of the books I've read recently as I've tried to become more conversant in all of this, as I think about how to move the NATO Alliance forward in the world of cyber. Some of them are quite well known. Toffler's *The Third Way*. If you have not read that in a while, and I had not, it is well worth going back and reading. It is unfolding in front of us. *The Cuckoo's Egg* is an old book but is a very vivid way to understand it. It's a true story about what we would today think of as….. *The Next World War* – computers; this really focuses on the cyber conflict piece of this. And *Ender's Game*. If you're not familiar with it, it's on all of the military reading lists. It's a very good science fiction novel that helps bring focus on this cyber world as we sail into it.

But books aren't what this is all about, right? Where you really ought to be is in these – in the websites, in the magazines, as in the on-line versions of these magazines where you'll really find the good stuff. Proceedings website, the U.S. Naval Institute website that Mary Ripley runs, is full of amazing blog posts. *Small Wars Journal* is dealing with this. We've got to use our communication means to exchange ideas, and I believe that by starting with a base from reading and study and then moving into the exchange of ideas, we can then begin to most properly address the challenges in this world.

My thesis for you today is that if we're going to address cyber, we need to do it internationally, we need to do it interagency, and we need to do it private/public. So I'll talk a little I ll about those three things. This is a photograph taken in Bosnia- Herzegovina where my command, U.S. European Command, last summer held an exercise called Combined Endeavor. Many of you were part of this as contractors in some way or another. We had thousands of people connected all over Europe, again centered out of Bosnia-Herzegovina. The three civilians standing next to me are the three tri-presidents. And we focused a great deal on computer defense. So internationalizing this, although incredibly complicated, is absolutely necessary.

Within NATO we've taken the first step to stand up this organization, the Cooperative Cyber Defense Center of Excellence. We decided to put it in Estonia because we felt there's a country that has experienced this. So we are beginning to put together an international center within the NATO context to begin looking

at cyber. And that needs and deserves our support from back here in the United States as well. So that international piece is crucially important.

We also have to get right the interagency piece of this. I very deliberately, in putting these icons of all the different interagency actors, have put the Department of Homeland Security at the top. We need to understand inside the uniformed military that we are not the drivers in this. We are merely part of the team, and we are there in many ways to support other interagency actors. The good news is in the Department of Defense we have resources. We have brilliant people like Keith Alexander, head of the National Security Agency, who is nominated to go forward as the head of our first cyber command. We can be y very supportive. But we need to understand cyber security in the larger interagency context, and we need to build a joint interagency task force and this U.S. CERT is the beginning of that. We've have great success with this joint interagency task force in Key West which focuses on counternarcotics. I would argue that model should be applied in this world of cyber security and indeed in cyber space itself.

That to me is the question we must answer – how we get our interagency together and focused. And again, I would advocate strongly for a joint task force with the DOD piece being supportive of it. And it's much bigger than the interagency. So if we agree that it's international and it's interagency, a lot of you ought to be recognizing those logos. They're the ones floating around in the rafters here. You are a big part of this, every one of you. And I believe that that nexus of private/public cooperation is how we first must understand this and then we must b i t l it Thi t l i i t b th llh d d k l ti begin to solve it. This truly is going to be the all-hands-on-deck evolution.

Let me talk a little bit more about strategic connections. Not strategic communication, I want to talk about strategic connections. I am a believer in the use of social networks to do this. They are extraordinary and powerful. We are seeing today, to give you one small example – in Haiti, where the language is not French, the language is Creole which is a very difficult language to understand unless you're a Creole speaker. We're finding that in doing our relief efforts in Haiti, we're getting text messages from all around the island but they're in Creole. We are using Facebook to connect with Creole speakers to get the translations, and that is being operated out of a network in a box called STAR-TIDES which you can see, I mentioned it earlier, down the way here. This use of social network is high potential. It is like the beach at Kitty Hawk right now. It's just the beginning, and the potential and the use of it are difficult for us to imagine yet. I'll give you one last example of why it really works. I was in a small venue in London giving a speech several months ago to maybe 100 people – a small group, I thought worth doing but not a big crowd. I mentioned, as I often do, *hey I'm on Facebook, friend me*. (I invite all of you to friend me, by the way.) So a reporter who was there picked that up and wrote kind of

a funny story that said *NATO Commander Needs Friends*. It was not a big seller; it was on the AP wire and it got picked up in two countries – Finland and Indonesia. The next day I got hundreds of friend requests from Finns and Indonesians. And the basic tenor of it was: *Dear Admiral, I hear you need friends. What is NATO? I will be your friend.* That's a funny story, but if you think about it, it's the power of social networking. You are reaching out to people who don't know you, don't understand what you're doing, and you then have the opportunity to explain it and have a dialogue with them. And I have had an extremely rich dialogue in particular with the Finns, who are not in NATO, about their security situation. It becomes a back and a forth, and a means of strategically connecting – strategic connections.

And cryptology professionals in the U.S. government. I'll refrain from all the nerd jokes I could go into, but it's 15,000 brilliant cryptologists and intelligence professionals who can use a Facebook-like application, A-Space, to find each other, to connect. Because the people who are doing, for example, counter-terrorism work at U.S. Southern Command with the FARC in counternarcotics want to be able to find who else is working on counter-narcotics in an insurgency. Hello, Afghanistan. And that connection allows them g to quickly move through to build groups, to build advocacy for ideas and presentations using this idea of A-Space. It's on SIPRNet; we need a NIPRNet version of this. This is also something industry can help us with. How do we build social network-like capability into the NIPRNet that could then be used to allow us this strategic connections piece.

How many people here have an iPhone? A lot, right? What do you love about your iPhone? You love your applications. They're free. They allow you to do all kinds of cool things. Why don't I have that within DOD, within the dot mil world? Think about the power in those kind of applications that could be relatively easily pushed or pulled into your command issue blackberry or iPhone or whatever – I'm not advocating any commercial solution here. But I do believe we need to look at this idea of applications. And how are applications built? They're done typically by people in a Wikipedia-like fashion populating the Internet with them, and then we effectively trade them. It's a marketplace. So how can we migrate to an application-like capability that we can use in the security dimension? I think that's an important part of navigating in cyber space that industry can help us with.

I talked before about Afghanistan. This is the image I want to get rid of. This is how we were paying the Afghan National Police two years ago. They were standing in long lines getting paper currency; corruption was a big part of the problem. Today we're going to help them, we're doing it, to skip this brick and mortar step. So there are practical applications in the battlefield, if you will, that are part of this cyber space, cyber sea in which we sail.

Telemedicine. Another rich and fruitful area that we can cultivate in this cyber sea. I don't have time to go into all of this, but I worked this very hard at U.S. Southern Command. It is an area in which what's happening in Haiti today has great applicability And the thing we can applicability. assure ourselves as we go forward is that this ability to move medicine and medical technologies rapidly across the Internet, across the cyber sea, is going to be vital for us going forward.

Terrain mapping. This is an application, a fairly simple one, that puts an actual photograph of terrain and then superimposes important navigational function on top of it, plugs into GPS, and allows our folks to land orienteer much more quickly. This is the type of solution that we're looking for….

Now, a lot of people comment to me on my resemblance to Brad Pitt. It's been a problem for me for the last ten years or so. I go somewhere, people think it's Brad Pitt. I put this up here to say facial recognition. It is so powerful in the counter insurgency zone. I want our folks to be able to pull out their blackberry, their iPhone equivalent and hold it up and use it equivalent, for facial recognition to differentiate between similar looking people like that. I think that's another area that we could use your help in.

Has anybody seen the movie *Minority Report*? It's an absolutely terrific film. If you haven't seen it, in terms of thinking about the near future I commend it to you. Tom Cruise plays the lead; he plays a police officer in a period of time that's indistinct but maybe ten, fifteen, twenty years into the future. This is a scene from it It's it. It s the use of these kind of technologies that allow us to use virtual display and pull information forward, push less important information back, to move it, to correlate it. This is a very powerful potential technology and can be used as we seek to understand networks in particular as we go forward into the future.

Let me give you a practical example as I said I would. This is Iron Key. It's a thumb drive. About a year ago in DOD we had a bad event where a lot of our computers were contaminated by the use of these thumb drives. This is a good-news story with Iron Key. Industry and the government created a well encrypted, protected and absolutely unbreakable thumb drive. That's what we need. We need practical solutions that can go in our pockets that are encrypted, that therefore allow us to move large amounts of data without contaminating our systems. This is where all of you can help us with your ideas and your energy.

This guy is my hero. I hope you get a chance to hear him speak about this cyber world at some point. Keith Alexander, the head of the National Security Agency. He is brilliant. He is balanced. He has a great sense of humour. He talks and thinks

constantly about this world, and I commend his speeches to you. If you want to learn more about this, they are widely available on the Web. A great deal of my thinking has been refined and assisted by my conversations with Keith Alexander and I fully credit him with a great deal of what I'm trying to communicate today.

Let me conclude with a couple of overarching thoughts about where we need to go with all this. In the end, this is what we must become in cyber space. And we are not there. We need to be like a cheetah. This is the fastest living thing on earth. It can go from zero to 70 miles an hour in three seconds with burst speeds higher than that It is that. purely optimized for its function – speed, it is incredibly precise, it is incredibly agile, and yet it is balanced. If you look at it, you see the genius of evolution. Look at the tail of the cheetah. You would think, evolution, if it wanted something to be really fast it wouldn't have a tail, or maybe just a little bobtail. The cheetah has a big, huge tail. Why is that? For balance. It gives it balance. It's what permits it to turn and be so agile. And that's what we need. To me, the image is the balance. It's finding the right turn of the rheostat between the need for open, socially networked connective technologies. and we need to balance that with protecting our networks. We have to be able to do both. We can't act as though life is an on and-off switch, because life is not an on-and-off switch. Life is a rheostat. We all know that from our personal lives. We need to find that balance, like the tail of the cheetah, that allows us to be stable even as we are fast and agile in this cyber sea.

There are great minds who are helping us every day with this. There's four generations of people who have thought about this. Upper left: Tom Watson, IBM. One-word model of IBM: Think. Think. That's what we all need to be doing. Bill Gates needs no introduction; as he himself says, he is the most successful guy ever to drop out of Harvard. He is an iconic American figure, in my view, who has helped move us to this next generation. The two guys g g y with the red screen there, does anybody recognize them? The founders of Google. And who is that guy in the lower right? He's a billionaire. He invented Facebook. Four generations. They all live up to Tom Watson: Think.

I started this talk by using an image of the cyber sea. I hope you'll permit me that metaphor as a Navy guy I've seen a few guy. I ve days at sea in my life. I will tell you if we think about this medium of the cyber world, it is interesting to contemplate the comparisons with the sea as follows. It has taken mankind two or three thousand years to sort out how we operate and sail at sea. Over the course of two thousand years, at sea we have gradually created international law, we've created bouy systems, we've created global navigation nets, we've generated charts. We've laid out a system. And in the 1980s the international community came together in the largest negotiating project in the history of mankind and created the Law of the Sea treaty. [160] signatories, took ten years to negotiate, extremely complex document, it's […] thick. It lays out the rules.

Now think about that in the cyber sea. We've been in the cyber sea, we've been underway for 20 years maybe, in a real sense maybe 10. And in the cyber sea we don't have those buoys yet. We don't have those charts. We don't even have the basic norms of behaviour. We don't know what the rules are in the cyber sea and the cyber world. The bad news is, we don't have 1,000 years to figure it out. Think back on the speed of change from that Radio Shack Tandy computer to the iPAD. Think about that ramp up in connections to the Internet: in 1984 1,000; in 1992 a million; today a billion. We're running out of time. And we need to generate these norms, these approaches. We need to understand and begin to at least have a dialogue about this cyber sea in which we're sailing.

So my thesis for you today is as you go about your work in industry, helping defense and helping the interagency, think about this cyber sea and think how you can help tame it. Because it is still an outlaw sea. And we need to understand how to bring it together. We must do that internationally, interagency, private/public, and we've got to do it by strategically connecting.

Last slide: Wikipedia. We all use this every day, maybe 15 or 20 times a day at least. It is a terrific tool. It is an example of a very powerful vision. The vision of Wikipedia is a world in which every single human being can freely share the sum of all knowledge. My thought for you today is that you must help us bring together the sum of all ideas ideas, to help us to tame this outlaw sea in the cyber world. I hope I've given you a few ideas today. I look forward to seeing you out there in the cyber world. Friend me on Facebook, I need some friends. I thank you for your attention today. It's been a pleasure being with you.

Thank you very much.