REMARKS AT GEOINT SYMPOSIUM 2010

SPEAKER:
JOHN C. INGLIS,
DEPUTY DIRECTOR,
NATIONAL SECURITY AGENCY

THURSDAY, NOVEMBER 4, 2010
2:00 - 2:45PM
NEW ORLEANS, LOUISIANA

MR. INGLIS: As you know, I don't come here as an expert in GEOINT but I do come as a longtime fan, not just of GEOINT but the people who have been leading the transformation in it for so many years.

Many of you probably know that NSA's products were long ago regarded as top-secret communiqués that would arrive on sheets of white paper, all capital letters, with the occasional insertion of a latitude/longitude in lieu of a picture. I'm really glad that not many of you know what that means in this public setting. (Laughter.)

But we've come a long way and, stride for stride, I think that we're being paced by the National Geospatial Intelligence Agency because the domain that we live in is, frankly, converging. It's very much the same domain. And while we have distinguished authorities, distinguished capabilities that we render under those authorities, we're increasingly working in the same place.

What I'd like to do today, then, is to call out a little bit about how NSA sees the world through a domain called cyber space, but at the end of the day, I think you're going to find that I don't so much call this out as a domain that is separate in kind but rather one that is converging or being converged upon by the place where NGA does its work.

It's difficult to describe this domain in kind of plain English parlance that would make sense. So often this is something that is imponderable because we delve into it from so many different quarters; we see it from so many different lenses, and we're frankly so busy that it's really hard to understand what cyber space is in the main as opposed to the very narrow slice that you might then see.

I'll take a couple of whacks at this. You'll see that I perhaps describe this in a narrow frame of reference in the light of efficiencies that are taking place in Washington, D.C. That's not either unexpected or not well practiced because I think you'll see, increasingly, people in light of efficiencies saying, we're unique; we're irreplaceable; we're something that must be left alone or untouched.

But, frankly, one of the lessons that I've taken from NGA leadership over the years, beginning with my early introduction to then-Gen. Clapper in the early-2000 time period, is that the real leverage, the real breakthroughs are not to be found in those unique areas but rather in the areas that you hold in common, the places where you join, where one discipline can leverage, cross-cue, take advantage of the other, and that's where I'll then come to ground, so to speak, at the end of the talk.

Right up front, if we could go to the slides, this is a characterization of cyber space that is so often used kind of in the quick ins and outs in terms of what is it, and it's a view of cyber space back in 1995 when there were 16 million users on what was then called the Internet.

And I was very proud in those days to own my own computing device, something I had at home. It cost me about $2,500. I think I'd bought it five years prior. I was going to hold onto it

forever because that was a lot of money in those days. It operated at a whopping 4.77 megahertz. That was the speed of the internal processor.

And I was ever so proud that it had its own internal permanent storage. It had a five-megabyte hard drive. I have no idea what you could put on that; probably a picture in those days if you could get it into the computer. And it did in fact have a color screen. You could either choose yellow text or green text on a black background. There's a little switch to flip back and forth, but of course no pictures.

It was very secure. The only thing it connected to was the wall, to get 120 volts from the wall. (Laughter.) There was nothing else that could penetrate it. As I recall, I would spend my days essentially doing directory searches to determine what was on the computer, but nothing was ever on the computer since there was no way to get it in and out. (Laughter.)

Here we are in 2010 and we have this fuzz-ball characterization of the cyber space – or this might be a proper characterization of the Internet. There are 1.9 billion users attached to cyber space, or this representation of cyber space today. Of interest, there are 2.2 billion social network accounts.

Now, I'm not a great mathematician but the arithmetic for me would say that some of you have two accounts or more in that space, possibly three since I don't have one in that space. It's a place where there is an enormous quantity of information – and I'll characterize in a bit what perhaps are the further attributes of that space that define what our strategy must be, and in that respect I mean the strategy not just of an NSA that does its work in this space all day, every day, but an NSA and partners who are also operating in that space.

In order to describe what those attributes are, I'm going to take an NSA whack at this. You'll note that we've come a long way at NSA. This is in all caps. I've made an artful use of white space – (laughter) – but it is a text representation of the space.

I'd like to characterize first, from an NSA perspective, what we see in this space as the salient characteristics that then in turn define what the strategic equity in that space is, and in turn what our strategy has to be in order to affect the things that the nation would have us do.

Top of the list is the self-evident statement of there's an enormous increase in the data available in that space. Inside NSA we often say that's the volume, velocity, variety issue – an enormous quantity of information moving ever-faster and coming at us in very complex forms. But, frankly, it's about more than the literal speed.

What's changed since when I had that PC/AT at home is that this is a place where it's not just about transactions moving from one sanctuary to another; it's a place where you are permanently storing wealth and treasure.

Soon after my PC/AT I bought a Compaq that had Windows 3.1 on it. And I went to AT&T and got OneWorld and I hooked up at a whopping 56 kilobits right to the local provider and was able to actually do some meaningful things beyond storing recipes on the computer.

I remember one day I kind of found this song out there that I liked and I wanted to download this song. At 56 kilobits per second, it said that it was going to take somewhere between 20 and 40 minutes, so I simply set the device and then went off on my walk. When I came back, the thing had downloaded. It was on the computer. And when I had gotten that data, I did what everybody did in those days: I'd disconnect from the internet.

What I had done was to extract that song from some sanctuary out there on the other end of the Net and I'd actually use the medium of the Internet as a means to conduct a transaction from that sanctuary to my own sanctuary and then I cut it off. I was safe on my side. If anybody had any interest in that song, or maybe it was a financial transaction, it was safe because I had physical integrity on my side.

Now, however, if you deal on the Internet, so many times there's no physical instantiation of the thing you're dealing with. You're not extracting it from one sanctuary and moving it to another in that space. It's in that space –cyberspace-- all the time.

What little money I have I allocate across a number of banks. We call that diversity in the year 2010. And one of the banks that I have an account with is the bank of ING, no relation to Inglis. In that bank of ING, you can find lots of literature in publications, perhaps the occasional billboard, but you could crisscross the East Coast for the rest of your life and not find a brick-and-mortar instantiation of the bank of ING because its wealth and treasure – my wealth and treasure, my $262.27, is out there somewhere as ones and zeros in the Internet.

That first property, wealth and treasure stored in the Internet, actually sets up a very strategic equity for the nation, and certainly for NSA, which essentially says because wealth and treasure is in that space, then that in and of itself is a strategic equity of the United States and allies and it must be defended.

The second property is the property of convergence in all things. Now, in a literal sense that means that where once networks were physically discrete, separate from one another, they have, over time, converged to the point where the networks are massively interconnected. And, increasingly, the network that you might think you're on is not, in fact, a distinct network; it's merely a virtual network that sits on top of somebody else's network or tunnels through somebody else's network. Everything is connected to everything.

But this, too, has some strategic implications in terms of what that then means in setting up a strategy for what NSA must do in terms of how it behaves in that space or, more importantly, what it must do in that space in order to defend the national equities.

The first thing I would note is that if you're a user and you connect yourself to that space in the year 2010, you're probably delighted that when you do a Google search you can touch one of 1.9 billion possible sources of information. But the other end of that analogy holds true, which is that now, because you've connected to that, 1.9 billion things can connect to you, and that's not always what you would prefer. Not all of those are friendly. Not all of those are what they purport to be.

And not all of those are things that you would intentionally choose to connect to, and though increasingly you don't have a choice – it's the way we build this space is to simply connect for connection's sake as opposed to for resilience sake or for some purpose of achieving integrity.

The other thing that comes out of this particular property is that you will find other domains of interest – other domains of interest like financial markets or perhaps secrets that you might want to keep to yourself. They're personal issues that you want to share in communication with your bank of your congressman. They're perhaps things that you just want to tunnel through from one place to another, imagining the day when it was going from one sanctuary to another, but today of course most of it is permanently stored out there on the Internet.

And I would note that other domains are dependent upon the integrity, the resilience, the availability of this domain, and so it takes on an even greater issue in terms of how important is this domain? It's not something you could lop off and the others then retain their integrity or their resilience or their availability. That too is an issue for the nation.

The third property of this domain is the increasing rate of change, oftentimes considered in terms of technology change. And, to be sure, that roils at a fairly rapid rate. Moore's Law is still generally holding true in terms of the increase in the power with respect to the properties of the literal devices that we use to connect to or operate in this space.

But what's equally important is the change in practices, practices of people who make use of technology in ways that the originators hadn't imagined. That changes even faster than the technology itself. The technology changes perhaps every six to 18 months, and then lurking, loping along behind are the policies, the authorities, the laws, the constitutions that govern the rules on how humans should behave, not just in physical world – you and I sitting here facing each other in the city of New Orleans – but in this world as well.

And the irreconciliation, right, the lack of synchronization between those three activities that are changing in that space– the behaviors, the technology and the law – that's an issue as well that I have to take into account when I do my work in that space because I can never, ever, ever find myself on the wrong side of the law or the authority that I'm granted, but I find on occasion that in chasing the operational behaviors of adversaries or in terms of trying to manipulate the technologies that I'm authorized to manipulate, I run up against boundaries that are sometimes not intended or not expected.

What this leads to, the intuition that you get from kind of taking that perhaps coarse look at the space, is a strategy that begins to emerge if in fact you want to defend equities in that space and you want to conduct the business of foreign intelligence in that space, which is what NSA's principal charge is, those two being information assurance, a formal mission for us; and signals intelligence, a formal mission for us. You get to the point where if you understand those properties of the domain, you have to think about achieving integration at Net speed, principally because integration is required because you have all of these multiple technologies, multiple

behaviors, multiple disciplines being wielded in that space, and unless you have a multi-faceted way of considering the bits and shards and shreds, you can't possibly put that together in terms of finding and fixing things in that space that you would then do something about.

And you have to do it at Net speed because that's the inexorable reality of the domain. The domain will not wait for you to step out, make a decision at human speed, then step back in and chase something that happened in milliseconds when you're now hours or days later.

The second part, though, the "empower all parts of the enterprise" is just a fancy way of saying that a hub-and-spoke system is no longer appropriate. NSA, in terms of its fundamental operations, 20 years ago arguably was a hub-and-spoke apparatus, much like AT&T, the telephone system was a hub-and-spoke apparatus, dumb devices at the edge – I'm talking about technology – dumb devices at the edge that would essentially be the things that would either communicate or send information, and the smarts at a switching center at the middle, at the center, the literal center of the enterprise.

That's the way AT&T did it. We, mirroring that in terms of how we would then deploy our sensors and deploy the kind of logic that would control those sensors, similarly came up with a hub-and-spoke system.

Now what you have, though, if you're chasing a network is the necessary ability of the devices, the sensors, to actually have a lot of autonomous logic or power at the edge such that they can discern something or relevance, take advantage of that thing at the edge without consulting with the center, without consulting with headquarters, and that's just the technology aspect of it.

What's more important still is to empower your people so that people, no matter where they are in your system, can take advantage of some insight, some knowledge that they've just gained, make a change, make a contribution, essentially posture a question that then the enterprise will immediately answer without having to seek permission of the headquarters.

But this introduces a very fundamental issue for the National Security Agency, or anybody else that would do business in this space, which is that it's not enough to simply get the job done, say signals intelligence. It's not enough to just do that.

I have to do it exactly the right way, which means that if I'm going to give my people some discretion in terms of the authority that they would have at the edge of the enterprise or anyplace that they might show up in the enterprise, I have to make absolutely sure that they know what the principles, the laws, the policies are and that they follow those with a relentless focus so that we get the job done in exactly the right way, not just with exactly the right outcome. That's a really big deal, and that then informs that culture because it needs to be as much a part of the solution as anything else.

With that said, I'm now going to take a different tack on this. I'm going to learn my lesson and say that perhaps, from an NGA perspective, you might look at this in a slightly different way, because while the intuition that informed those attributes of the domain, and

perhaps the elements of the strategic response, were I think true enough, it's still hard to visualize how would you put your arms around this; how would you actually attach yourself to it, how would you do meaningful work in that domain if you didn't know where or what you would attach yourself to.

And so this picture you see on the screen is essentially borrowed from the sort of approach that an NGA would take, to say let's perhaps characterize this in the visual form. There's a layer that constitutes cyber space that really is the wires, the cables, the RF runs, along which pathways the information literally flows from place to place, and you might think of that in terms of being a layer in a larger model.

On top of that, you might then imagine that there is a network logic layer. That is the layer that determines whether it flows from A to B through C or perhaps through D - it's the layer that determines the paths information follows through the pipes and wires around the globe. Now, it being dark on the backside of the planet at this moment in time, it may defy intuition that a lot of communications that people are trying to send from New York to San Francisco would have the easiest path by going perhaps across the dark side of the planet.

Unless you understood that this logic layer is always trying to smooth those data flows around the globe, you might think that the shortest distance between two points is defined by geography as opposed to by network topology. But this layer has everything to do with why the domain is so befuddling, why it runs roughshod over geography because it's actually trying to affect a different form of efficiency and effectiveness.

On top of that, you have another layer containing the devices that literally are connected to the network, the devices that act as surrogates for human beings. These three layers together constitute a really important place for the National Security Agency in terms of either doing its defensive mission or its foreign intelligence mission.

If we were to think about this space --"cyberspace"-- in NSA terms, we could be quite happy sandwiched between these three layers, essentially finding and fixing things in that space, deriving value from things in that space, or perhaps defending things in that space. But at the end of the day, our customers want to know something more than what happened at a certain IP address or what happened associated with a certain device.

They want to know where it happened on the planet Earth because that's where human activity has its nexus. And so, the geographic layer is absolutely essential to this model. They also want to know which human you can attribute this activity to, and so it's important to put a top layer on there, comprised of the human beings for which this domain exists in the first place, such that you can then, with all of those layers in mind, integrate the various perspectives, disciples, capacities you have to make sense of this vertically, from geography to human and back again.

The challenge in cyber space, of course, is going to be that one human being can have multiple representations in this space because they can attach to multiple devices, can take multiple paths, show up as multiple instantiations of activity on the planet Earth, and that can

change over time. From one moment to the next, that same person could take a very different representation in that same space. Hence, you have 1.9 billion users but 2.2 billion social network accounts.

And, finally, for this reason NSA cannot thrive, cannot essentially prosper in that space alone. It must have the material assistance of an NGA in order to map into the geographic layer or to understand at the human layer how we attribute these actions. Attribution and geolocation are essential properties of the services we would deliver to our customers because they must geolocate and attribute these activities in order to have effect with all the other instruments of national power that we're informing.

Having said that, the next thing I'd like to talk a little bit about is collaboration because integration is a watchword for us. I talked about integration at Net speed. It is a watchword for us at the National Security Agency but, more importantly, collaboration is simply the human equivalent of what Director Clapper mentioned earlier as the strategy element that he's concentrating most on – integration.

In thinking about that, I thought about a few years ago when I was introduced to this in a very compelling way by then-Gen. Clapper, who was the director of the NGA. It was just after the 2001 attacks, (9/11), and Director Clapper had suggested that NSA and NGA form what we then called the geocell. It was an activity where we could put analysts from the respective organizations side by side and have them essentially participate in what was called the connection of the dots.

Now, the notion of connecting dots actually spoke to a bias for integration that I think had the following, I think, benefit, but also the following deficiency: The bias was that there were all sorts of dots that had been produced that would constitute a rich mosaic of a picture if only somebody got together and figured out how to combine them into a single common picture.

The deficiency in that, though, was the presumption that each organization, each stovepipe that had the expertise and the ability to create dots, was sufficient, in the depths of that particular stovepipe, to create all the dots that were necessary unto themselves. That NGA, CIA, NSA, DIA would all happily produce dots, push them to the top of those respective stovepipes, and the task that then remained was to then array those dots into a particular picture.

Of course, that wasn't at all the case because inside each of those stovepipes there remained shards, shreds, hunches, things that never saw the light of day because there wasn't enough information to make sense of it and push it above a reporting threshold.

So what happened in the geocell was something near miraculous, which is the two analysts sitting side by side didn't so much compare the dots that they already had, but they drove each other to actually make sense of the half dots, the shards, the shreds, the nuances that they already had in hand, the hunches.

So what you found is that you were driving collection as much as you were driving post-production analysis because you'd put these people side by side. One analyst would lean to the

other and say, we're hearing something that's very interesting in this neck of the woods, something that's anomalous, something that is a concern to us. What are you seeing? And the other analyst would say, we're not looking there.

All of a sudden you would bring to bear an aperture or an asset to look there and you would put together the rest of the story. The integration in the bowels of those stovepipes was the miraculous breakthrough of the integration begetting collaboration between those two organizations.

Now, another challenge in integration sometimes is that people think of it in simply engineering terms, that if we only devised the right systems, that the integration could happen autonomously or without benefit of human intervention. And of course the example I just showed is more about the ethos, the culture of the two sides than it is about anything else.

But the other downside sometimes of "integration as the ruthless focus" is that you want to make sure integration is really about trying to take advantage of stovepipes, not replacing stovepipes because the stovepipes, again, as Director Clapper said earlier this week, are essential and valuable in their own right. That's where a depth of expertise comes from so that you can then, when you integrate that at all levels of the respective organizations, achieve something that no homogenized version of those skill sets ever could.

The services have practiced this form of integration for a long time under Goldwater-Nichols, namely that they retained the stovepipes – which are the Army, Air Force, Navy, Marines and Coast Guard. That's where depth of expertise comes from. You want somebody to fly an F-16 over your battlefield, you would hope that they have been to pilot training and that they've actually had a few years in the cockpit, but you want them to know that unless they can do that in a joint world, that skill is of no value whatsoever.

So what I would like to roll through, then, are some lessons extracted from that particular experience about what constitutes collaboration, and perhaps then talk about what is necessary from this point forward to effect the sort of collaboration that all the leaders this week have been speaking about.

The first foundation for collaboration is of course "common cause." You have to have something that is worth collaborating about. And in the case of the intelligence and security community, we get that for free. Our nation's security is the compelling common cause. That's there all day, every day.

But the second issue of course is leadership. Does leadership point out the common ground? Do they describe that in the common terms? Do they describe the collective charge? Or do they focus and narrowly think about the individual charge, assuming that we will again kind of simply combine these bits, these parts in post-production? It's not an engineering activity, and if it is not an engineering activity, then the culture has to be led by leadership.

The third artifact that is essential is personal relationships. The bottom line is that the personal relationships matter and they matter greatly. I mention this by way of saying that unless

that physical intimacy had been created in that geocell that I spoke to, I suspect there wouldn't have been nearly the sort of profound breakthrough that I experienced when I watched the geocell begin to change two organizations much for the better.

Once formed those personal relationships can then be sustained at a distance by virtue of technology across at-a-distance relationships. But the point remains that at some point people have to know one another, they have to actually have a relationship with one another, because otherwise they're not able to ask questions that the other side would understand. They will talk past one another.

In testimonials that I've heard across the years from various analysts looking to collaborate without the benefit of a personal relationship, they ask the wrong question, give the wrong answer simply because they don't know enough about what the other side's possibilities are or what the other side's true needs are because they lack that personal relationship. Absent the personal relationship, all the technology in the world, all the common cause in the world isn't enough to overwhelm that particular hump.

And the last characteristic that I would put up here is in fact infrastructure – infrastructure that, when the flesh or the spirit is willing, makes it possible to then pick up the phone or to effect a relationship or to effect a transfer of information across infrastructure, whether it's technical or process or doctrinally oriented. That's an absolutely essential component of it as well.

Oftentimes when people talk about collaboration, they think, why is this so hard? Why isn't it as easy as it is, say, in the middle of a crisis?

Well, I would remind us that in the middle of a crisis you don't need leadership or infrastructure. People will go to great lengths to overwhelm a poor infrastructure, and regardless of what the leaders might say in the middle of a crisis, people see the common cause as the compelling, overwhelming circumstance. And they get together in coffee bars or in basements or in the parking lot of the Pentagon to get the job done.

But that's not what you want to sustain, this sense of crisis – perhaps a sense of urgency but not a sense of crisis – because our fundamental charge is to not have a crisis; it's actually to avert the crisis. We're not here to prepare for the next 911 or prepare for the next Pearl Harbor; we're here to actually avert that.

And so you want to get to the point where all four of these elements are in fact the foundation and they are in fact alive and well in creating the culture and the infrastructure necessary to achieve collaboration.

My view of what I've seen NGA do in terms of how it deploys its people, how it designs its infrastructure, how it essentially defines the culture of its relationship with other organizations, whether they are partner organizations like an NSA or customer organizations, those that we ultimately are responsible to deliver our services to, is that they have practiced that to a fine art. And, frankly, from an NSA perspective, there's much more that we can learn from

NGA, not least of which is the use of pictures in lieu of text, but certainly in terms of the ethos and the culture that derives from that.

Having said all of that, that's essentially my basis for why I'm here. This relationship is important enough that I would come down, you know, even if it meant I had to cross the country in a single day and back to participate in something like this, because what I see in terms of what NGA is doing is something that is trailblazing, not for the GEOINT discipline but for the INT discipline, because at the end of the day that's what we're here to do is to apply our various and respective depths of expertise to the common cause, which is the nation's security, and I see that it is working very well in terms of how NGA has laid that out.

I see that I have about 20 minutes left for questions. I would be delighted to take any and all questions at this time, wherever you would have the conversation go. Jeff? (Applause.)

MODERATOR: Chris, thank you. I think the framework from where you began the conversation where all of America realized that the use of a personal computer at home was sorting recipes and nobody has yet gotten there – some of the audience are frustrated by the fact that – the seniors that are of sort of our age group will say, I understand that there's the Wild West of this Internet, but I believe I can continue to connect, do my job and disconnect, and that provides a lot of protection. Do you have any comment on how we drive a culture change that accommodates the culture change you've gone through, watching from the inside?

MR. INGLIS: Yeah, so I think that's a great question. I would say that, speaking for NSA – many of you know that if you ask NSA a question we will generally start in the middle of our story. It's a little bit worse than if you asked the man what time it is and he describes how to build the watch.

We will describe an implementation or a response, right, to the question you've asked something about as opposed to start in the formative period to perhaps say, you know, here's why I would do that, or here's what's at stake, which would cause me to do why I would do that, or perhaps here's how the domain itself actually operates.

To the extent that senior policymakers, whether they're in the executive or legislative branch, or sometimes in the judicial branch, don't understand the space such that they could then help frame it, guide it, govern it, I think that that's a material responsibility that is attributable to us. If we do understand that space and we know perhaps what the right response or what the equities of consequence are in that space, it behooves us to put that in terms that they can understand, to explain not just the response but the compelling cause or the fundamental principles that govern the space.

So I think we collectively then take a charge to help them understand that, without being patronizing and without being perhaps overly serving in the roles of marketers about this all about trying to get the next $500 million for whatever the pet project might be. That will mean a lot of time around tables with sleeves rolled up.

Our experience has been that policymakers are willing to commit the time and attention, but we need to come to the table with something that is in English and plain and simple but compelling to get quickly to the fundamentals of what's going on in that space, else they're going to get to the point where they will ignore the reality and simply say, I'm just going to disconnect from the space because it's a threat-oriented space or it's too confusing, not knowing that it's impossible to disconnect from that space. It's too late for that.

MODERATOR: Thank you. Continuing along those lines, it's clear we turn to the National Security Agency for expertise on a very complex subject with the ones and zeros flying through cyber space.

When I look at nation states and how nation states protect the commerce, to your point, can you describe the relationship between NSA and the Department of Homeland Security and Customs? We have customs at the border that protects the border, but the border in cyber is not the border – you get it.

MR. INGLIS: Yes, I spoke briefly about a national equity, and I frankly think it's an international equity in cyber space, that we have collectively stored wealth and treasure in that space and it must be defended. I didn't say much about whose job it is to defend that, and that must be, in a coalition format, everybody's job.

There's going to be a responsibility borne by users to essentially manage their own affairs in that space as well as they would perhaps manage articles of value that they have in the physical world. There's going to be a responsibility for network managers to essentially make it possible for that space to be defended. There's going to be a responsibility for various government organizations to exercise their lawfully designated authorities to perhaps set the rules and to work with industry and to establish the coalitions necessary to make that space both defensible and well defended.

In the kind of realm of cyber space or in the realm of the Internet, perhaps as a subset of that, the responsibility for defending dotmil is clearly a military responsibility. The responsibility for defending dotgov is a Department of Homeland Security responsibility.

They therefore are necessarily on point, and by further extension, because DHS has the responsibility of dealing with the private sector, are responsible for engaging various and sundry of those elements of the private sector to help effect a transfer of expertise and a transfer of expectation from the government to the private sector. But most of the burden in this space is going to be borne by the private sector because it's the private sector that's building and transforming that space as we speak.

That being said, NSA and the Department of Defense, organizations like NGA, have an enormous experience in dealing with the issues in this space, whether it's a volume, velocity, variety issue, whether it's rendering bits into plain text. We have some contribution that we can and must make, not simply for the defense of dotmil but for the defense of dotgov or for the defense of dotcom.

It's not something that we can and will force as a matter of policy, but it is something that we must make available. The National Security Agency, for example, under what's called the National Security Directive No. 42, has the authority and the responsibility of providing technical expertise to other members of the government who asked for that.

We are, on a routine basis, providing expertise to the Department of Homeland Security so that they can properly execute their responsibility. You may have seen in the press not long ago that the Department of Defense and the Department of Homeland Security have formed what's called a joint coordination element to physically put people side by side, respecting and retaining the authorities that are unique and distinct but making sure that they had that virtue of collaboration that I spoke about earlier, which is a face-to-face relationship where they can better understand what they might do for one another to help them effect their responsibilities, which cuts across a space where they all live in the same place, where they all work in a common space.

MODERATOR: Thank you. Your charts of layers I think is a very helpful construct. If you stand back from it half a mile away, it will sort of scream out "infrastructure." And so I see layers and layers and layers of infrastructure. We talk about cyber space almost like it's independent of infrastructure, but certainly in the news the industrial controllers, when infrastructure, whether it's the economic side or the industrial manufacturing side, there's a huge convergence there.

MR. INGLIS: There is.

MODERATOR: Is there new thinking that's going to take place?

MR. INGLIS: I think there must be. That's not going to be something that's dictated by the government or by any one entity that's living in that space. So I think what you're going to have is in the near term, you know, do what we must in order to make the space more defensible.

Deputy Secretary of Defense Bill Lynn, not long ago in the Foreign Affairs journal, published an article which described the Department of Defense's approach, which was to insure that we did what we should in terms of establishing the software and the hardware properties of the devices that are already in that network to make sure that they are tuned to the point where they can be reasonably – we can be reasonably confident that we're taking advantage of the security properties they have.

We'll establish perimeter defenses so that we can insure that we're at the boundary between what might be perhaps a more integral network, dotmil, and the outside world to which we want to connect; an understanding of what's traversing that boundary so that we can understand perhaps which flows are inappropriate, which are appropriate, and manage that accordingly; that we will hunt on our networks appropriately and within the full scope of the law, but to understand the threats present on our networks and to mitigate and/or remove them so our users can conduct their business with high confidence of integrity, availability, and confidentiality.

(END OF RECORDED Q&A)