SPEAKER:

DR. ERIC HASELTINE, ASSOCIATE DIRECTOR OF NATIONAL INTELLIGENCE FOR SCIENCE AND TECHNOLOGY

AUGUST 24, 2006

(Applause.)

DR. ERIC HASELTINE: Well, thank you. It's a great honor to be here today. I wanted to start off by asking a question to the group: How many of you know who Niels Bohr is? Can someone yell out who he is?

Physicist, right? That kind of solar-system view of the atom was due to him, the Copenhagen model of quantum mechanics. And I'm here to tell you this morning that Dr. Bohr was wrong, not because of the solar-system model, which is a little bit over simplified, not because of the Copenhagen model, which some will view is not correct, but because of a Yogi Berra-ish statement he made, which said that, "Prediction is difficult, especially of the future."

I would say that prediction is not difficult. I would say that prediction is actually quite easy, and I'm here to show you how easy it is, that I think our future is in some ways crystal clear – a little disturbing, but clear.

So what I'm going to do is give you a perspective from the crow's nest to tell you what is on the horizon and over the horizon. And hopefully on the horizon doesn't mean, like, a painting where the technology on the horizon stays on the horizon forever. Like artificial intelligence, for example; it's the technology of the future and remains so.

What I'm going to do, building on this metaphor of the crow's nest, is talk about two facets: navigation, which is, in general, where it is that we need to go for information sharing, and then steering, which is how do we get there? And this is the vision-to-reality piece.

Where we need to go: First, we have to go back. What we see here is a graphical representation of the problem, that there is an inescapable law of physics that says the more you share, the less secure you are. The whole notion of a shared secret is an oxymoron. And privacy and security are really two

different elements of the same thing, which is how do you give the information to people who need it and should have it and keep it from those who don't?

What we need to do, simply stated, is to move from the curve that is red to the curve that is green, which is to say we can't get around physics; the more we share, the less secure we are going to be. But for a given level of sharing, we need to have greater security, and for a given level of security, we have to have more sharing.

Now, you may say, well, how does one accomplish this? Let me give you an example. Let us suppose – and you have heard about XML tagging and marking and measuring of data and watching what happens to it. And we'll talk about this more later. But suppose you could do that; suppose every single piece of information was marked and watched so that you could know who is looking at it, and based on who is looking at it, do Amazonish-like things like push the information to analysts or to end users without them having to ask for it so they don't have to play 20 questions; it comes to them. That is better sharing.

It's also better sharing in that you can start looking at patterns of behavior and understanding what is really useful and what is not useful. It's also more secure because you know where your children are at night; you know what is happening to your data; you know whether there are anomalies. So in theory at least, there are technologies that will push this curve out, and that is our challenge.

How do we do it? Well, I would submit that there are two pillars. One is what I call the technology of being able to share, and the other is the psychology of getting people to want to share. I know a lot of you are probably guilty of saying the thing that I keep telling my bosses, which I always hate to say given that I'm the high priest of technology for the intelligence community. And it's four words: It's not the technology. How many of you have said that? Right. We all have because it's true.

The technology for information sharing is there today. We all know that, but we posit some obstructionist who is stopping it. Gil Decker, who talked to me before I took this job – he was the assistant secretary of the Army. And he put his arm around me, and he said, Eric, in the national security establishment, you can think of it as plumbing. And there are two kinds of fixtures in plumbing. There is valve and pumps, and there a whole lot more valves than there are pumps. And that is kind of what we technologists think, that it really isn't our fault; it is somebody with a brain there on the right that is causing the problem.

So what I'm going to do is I'm going to drill down into the future, and talk about where bitware (sp) is going where it is going places that are very significant for information sharing. And then I'm going to talk about the wetware side. The wetware side is no problem predicting that because all you have to do is look at how human nature is today, and I think you would be on pretty solid ground saying that is the way human nature is going to be in the future. So it is not so much prediction as it is extrapolation of taking human nature as it is today and extrapolating it into the future where it intersects technology.

The way I am going to approach the bitware problem – and bitware, by the way, encompasses software, hardware, firmware, any kind of ware that isn't neurons, although down the road, that

distinction, too, may blur, as you will see. But I believe there are certain forces of nature, Moore's law, Metcalfe law, various other laws that make the future at least out to the next 10 years very predictable.

And the core driver of course is Moore's law that says that every 18 months, you get a doubling of performance for a given footprint in price or you get a halving of price for the same level of performance. And the semi-conductor industry projects that even with all of the problems and having to go to multiple cores and all of that, we still see that trend continuing at least into 2016. And then I'm going to say what it means for secure sharing from a pure technical point of view.

So the first law of nature is that dumb things get smarter, which is – and example. Think of the watch. The watch started off as a bunch of gears. And it was smart to a point; it knew what time it was twice a day, even if it was stopped, but knew better than that if it wasn't stopped. Today a watch is a computer. The other interesting thing is the proportion of software that is in your watch, your car, your refrigerator – and with RFIDs, soon every single consumer thing that you buy is going to grow. And that software really is where the intelligence is.

Now, there is a really interesting implication of that which is worth a whole speech in itself, which is what does that imply for who we should be training and recruiting, and what does that imply for where the real value-add is. I'm going to put that aside because it's beyond the scope, but I think it's a profound implication that it doesn't matter what you're trying to do with technology, the proportion of that technology that is software is going to grow exponentially.

One implication of that is that if we look at the data itself, we talk about sharing information, let's take a microscope and actually look at that information in its actual physical form. In the evolution of information, we started off verbal, and then we migrated to the written word, then we migrated to the printed word, and so forth.

So let's start with paper. Paper was a dumb thing; it was just processed trees with some ink on it. Then, paper migrated into a Word document, and a Word document started off pretty dumb. But then you started getting macros and so forth, and then you have this innovation called hyperlink, and XML, and yadda, yadda, yadda, yadda.

So clearly what is happening is, just as the watch is getting smarter, so is the information itself. Now, some of you may recall Alan Kay, who was at Xerox PARC and then at Apple, and then at Disney, where I sat next to him for five years, and by osmoses, some of his brilliance seeped across into my dim-witted brain – that is the way he viewed it, anyhow. And he had a really interesting project that started off as hypercard and then became Squeak, and now it is something else.

But the basic idea, or one of the ideas behind it is that data are going to get very smart. He had a very interesting demonstration. And you might just guess at what – having been Apple, and Xerox PARC, and so forth, what his attitudes were towards Microsoft.

And so he had a very interesting demonstration with Squeak. He put a demonstration on where he loaded and executable/data file that had a footprint of a few megabites. That was it. And what that executable did was that it put Windows to sleep. It completely put Windows to sleep. And on the modern Vista-type machine, where you have privilege partition and mandatory access control, you

literally could have Windows put itself to sleep and have a series of concatenated micro-kernels pull themselves together and essentially be the OS of the system.

And essentially what he did was he had what we show here on the right, which is that he had all kinds of applications, texts, graphics, interactive, this, that, and the other, and they carried with them their own rendering and presentation layers, and their own micro-kernel. And he had a bunch of hobbyists, thousands of them all over the world, a lot of them in Germany, who imported this Squeak executable onto every conceivable kind of processor for free, literally thousands of different processors from pics (ph) all the way on up, to strong arms and AMBs and so forth. So it was a BM type of approach.

But what did it really mean? What it meant was for the first time, the data was not a victim of its rendering and its – in the rendering and presentations links. They did carry with it all of the intelligence that it needed to do it's thing.

So just imagine now that you have a piece of data and the data knows where it is, what machine it's operating on, who is looking at it, and it decides, unlike a Word file, which opens up to any old person – it decides do I want to open up, do I not want to open up? Do I want to transit this gateway? Do I not want to transit this gateway? That the intelligence moves into the data. And it gets back to my point about software: that the distinction between the data and the executable is rapidly going away, in fact, if it hasn't already gone away.

Another aspect of a dumb thing getting smarter is whatever it is that we have, it is going to know who is using it. Not only does it have its own Mac address and its own IP address, and its this and its that, but it's going to know who you are. And what is driving this is two large market forces that have nothing to do with our business; it has to do with – if any of you read the "One to One Future," the inexorable trend of all consumer devices to be a niche product – I mean, just think about if you are as old as I am and you used to go to the supermarket, how many different kinds of soda were there? There was Coke, there was Pepsi, there was 7-Up. Now, how many different kinds do you have? Now, you have got decaffeinated, cherry, diet, low-sodium, unobtainium Pepsi, next to – all of those things except caffeinated.

So that is a kind of a magnification, if you will, of consumer processes, and it all has to be based on who you are. So devices are going to know who is using them. They are also going to know where they are. They are going to have GPS or Rosum or some kind of thing in them that knows where they are to great granularity.

Now, the other thing about smart things, just like people who are arguably smart things and like to get connected to other people, so too do the devices made in their image what to get connected. So the trend in everything is if I have got a brain, I want to connect to other brains, and that is a trend that is continuing apace.

The interesting thing about this is let's look at RFID. And RFID kit today with some decent performance costs you about 75 cents. Moor's law says that it's going to cost about half a cent in 10 years for that same capability. Well, what that means is that these chips are going to get more and more ubiquitous, and also without reducing price so much, they are going to get more and more capable. So they are going to start talking to each other instead of some central system.

And so these dumb things that we are talking about that are getting smarter are going to get more connected with each other without ever having to get connected to some central process. What this means is a peer-to-peer world, a mesh world, which, by the way, poses profound implications for our business. If we do not know when a communication is happening because it's happening without any centralized monitoring control, what does that mean for us?

Another force of nature is that things are connected to go wireless. I think it gets down to the personalization thing. We want to have our experiences when we want, where we want, how we want. And I like EE Times. It is one of the articles, periodicals that I read very often because what I find is that they start discussing all of the standards wars, and when you know the standards wars are done – for example, the wars between Erickson and QUALCOMM on wireless protocols, you know that it is going to get real two to three years before it really does.

And what EE Times said about three years ago was that in this fight between the PDA, the pager, the DVD, the yadda, yadda, yadda, that the cell phone was going to be the winner. And that says that whether it's a cell phone or a PDA or a pager or an MP3 player, it becomes moot at some point. But the fact of the matter is that if you're talking about ubiquitous information sharing, by which I mean anywhere, anyone, anytime, exactly the way you want it – that appliance that I show there is going to be a pretty good approximation of how we are going to do that – then everything is going IP.

And this is an obvious statement, but the implication for us is that everything is going to be connected to everything else. That means these RFID chips that I was talking about, those things are going to be IP, guaranteed, and they are going to be able to talk to anything else. Now, there is some interesting implications of that for security.

Let's think about this: If you look at our adversary, big nation states, and you ask if you took an ohm meter and hooked up their air-gap network to our air-gap network, would you see current? The answer is you would. We are all swimming in the same bathtub, and that again has profound implications on both sides of our business.

By the way, it's not just our network; it's Starbucks; it's that RFID chip. Why do I think RFIDs are going to be ubiquitous? Because I came from Disney, which was a consumer-marketing-type company, and we realized that understanding the consumer deeply was really important.

And that led us to look at supermarkets. How many of you have supermarket discount cards? Do you know how much of your privacy you are giving up with those cards? Does anybody know? You are giving it all up. They know everything that you buy down last match, whatever. The stuff you get in your mailbox is very much determined by what you put when you scan your card. You know, they knew for example that there was a super-high correlation between the purchase of beer and diapers. (Laughter.) Right?

Now, that is not because men are all babies, as all of the women here know – (laughter) – that is because there was an interesting sociology which said, honey, would you go to the store? I have to change him; you go buy them. And honey goes to the store, and he has to buy diapers, and what else

does he buy? He buys beer. So if you buy a certain kind of beer, you're likely to get a direct mailing for pampers. (Laughter.) Okay?

And I'm not going to dwell on that much longer except to point out that what do you think the odds are – if I say to you, you, sir, that blue shirt that you're wearing. That blue shirt probably cost you about $40. Well, if you're a government employee, 20. It cost you $20. Would you take a discount at $5 if I allowed – if you allowed an RFID chip, which was used for inventory and supply chain management? After all, all products will have that in it because it will be less than half a cent. Would you allow that RFID chip to stay in there for a $5 discount?

You might not, but a lot of people would. And we know that because we know that almost everybody in this room essentially does the same thing with their supermarket cards today. And so that means that literally a dumb thing like a shirt, a tie is going to have an RFID, that these things are going to talk to each other, and all kinds of emergent behaviors like beer and diapers are going to come and be used. Well, what does this mean for our business? It means literally that everything is going to be connected to everything else, and I mean everything.

Here is an interesting thought. Alan Kay also said a word is worth one-thousandths of a picture. I'm not going to say any words. Here is something that I want to dwell on a little bit, and I think unfortunately it's going to be very hard to see this slide because I didn't realize – I guess you can't see it. What you would have seen if the slide had rendered properly is mirror curves. So imagine this; imagine on this access – this is what I call air PowerPoint. (Laughter.)

Imagine on this access you have – so let me see. I have got to reverse it here. On this access you have performance and on this access you have costs. And on this access you have time. What we know is that with Moor's law, you can ride one of two curves. You can ride the performance curve at the same cost and go like this. So every 18 months I can double the performance. The other thing you can do is you can hold the performance constant and ride the cost curve down. And what that would mean, for example, this morning I saw advertised a trayo (ph) device – $300, 300 megahertz, and 30 megabits.

So what that means is that in 10-and-a-half years, which is seven turns of Moor's law, you divide all of that by 128, or you multiply the performance by 128 on the performance side, or you divide the costs, which says that if you take $300 and divide it by 128, you get something a little north of two bucks. Or, if you take the performance, you get performance a little bit north of megahertz – excuse me, 40 gigahertz and memory of 40 gigabytes.

Now, does any of you really think that this device is going to be available, this exact device is going to be available for two bucks, this exact device? Of course not. Why? What is the margins on two bucks? Squat. So formally, greedy people like me who wanted to, you know, get you to pay us money. Excuse me – (laughter) – formerly intelligent people like me. You can see my little calculations on the back. That is what I was really intending to show you.

The point is of course you're not going to be able to buy this exact same thing for two bucks because there is no profit in it, and also by that time, all of those cool little things like cameras that look at your mouth and do voice recognition because looking at your mouth makes voice recognition better, bio ID, all of those things are going to be in there.

And what is really going to happen, instead of the cost curve coming down like this and the performance curve coming up like that, what you're going to see is both of those are going to stretch out. Okay, you're going to see a lot more performance, but not as much as you could have theoretically, and you're going to see a lot lower price for performance, but not as much as you theoretically could have had. And there are market forces and application forces that drive you that way.

And to just know that that is true, I bought my first Sanyo PC with CPM and DOS and all of that stuff, no Windows, just command line – you know, back in the early '80s. So, okay, that was, say, 25 years ago. So 25 – so maybe 15 or 16 turns of Moor's law. That was a $2,000 computer. Can you buy a PC today for two-the-16th less than 2,000? No. But the performance that you have is a lot more than my little CPM that later became DOS and so forth.

So I think the point I'm trying to make here is that in trying to predict the future, what we know is the theoretical performance is not what we are really going to get. But factoring all of that stuff in and boiling it all up and doing this, you want a prediction of the future? Here is a prediction of the future. Here is Haseltine's prediction of what will be available in 10-and-a-half years. So that means the end of 2016.

This device here with all of the new bells and whistles will cost less than $99, probably considerably less if you get a service plan. It may be free in a sense if you buy the service. You will have greater than 15 gigahertz CPU, greater than 15 gigabytes of RAM, and it will connected wirelessly, at least in urban areas at greater than 10 megabits per second. It will be smart. It will know who is operating. It will know where it is. The data in it will know whether to release the information based on – and what happens to the information that is shared will be recorded. It will support multi-user videoconferences for data and voice. It will be stealthy from a security standpoint. Because this is a public meeting, I will only briefly dwell on this point.

Just because you can have a secure pipeline that protects the bits all the way down to the screen and the microphone, you still have to worry about the analogue world in which electronic information and acoustic information and visual information still are radiated. And if you are in downtown Moscow, you may not want to have a terminal out there where everybody can see it and hear it. So what I'm trying to say is that there are some technologies that can solve that problem, and I'm not going to get into that. But, again, to go back to where I started this speech, it is not the technology that will stop that.

So what it all means is this, that there will be a very cheap platform that will enable you to securely share any information any time, anywhere, with anyone. That will be there. But – and it's a big but – who is going to make this stuff. Where is this thing physically going to be made? Where is the code physically going to be written? By whom? Which network will it send its information over? Who designed and built that network who owns that network, who supports that network? Question.

Okay, I want to shift to wetware because we all know – I think you're all thinking probably the same thing I'm thinking when I look at these marbles, right. By the way, I have to dwell and just make a point.

You heard in the biography that I was a human factors person. You're going to see more of this later in my speech, but my prediction is that as the percent of software grows in this kind of device, the percent of that software, which is devoted to making something which is very smart, the computer, interface to something that does not change and is sometimes not all that smart as human will grow. In other words, the piece of the value add that impedance matches the bitware to the wetware is going to grow exponentially, to the point where you'll have a little tiny bit of application being run with a huge user interface human factors piece. And that is I think something else about the value added. And I'll dwell on that in a moment.

So let's talk about motivation. There are two kinds of motivation I want to dwell on, and I don't think that we often think about these exactly in the way that I'm about to get into. There is extrinsic and intrinsic. Let me talk about extrinsic. I am guilty of being a behavioral scientist, neural scientist. And so I have this overly simple way of looking at behavior, and it goes like this: You get the behavior that you reward and you don't get the behavior that you punish. Now, to the degree that that gross generalization is true, if you're looking at the way we share or horde behavior today, you say however we're doing that must be a reflection of what we are rewarding and what we are punishing.

Someone once said complex problems require simple solutions, and very complex problems require very simple solutions. Well, duh. Maybe this is a simple solution. It's a four – it's a two-by-two matrix cell. We can reward sharing, but we may only get a piece of the action there. If we are still punishing sharing at the same time, you get into what the psychologists call an approach-avoidance conflict. Come here little doggy. Whack. That is approach avoidance.

So we have to do four things. We have to stop rewarding hording. We have to stop punishing sharing. We have to start rewarding sharing. And we have to start punishing hording. Now, I want to say here that it's not like we have a conscious strategy within the intelligence community to do all of the bad things here and not do all of the good things here.

Really what I'm trying to say here is that we have to constantly keep in front of us the challenge, the constant challenge of looking at this two-by-two matrix. There has been tremendous progress. I have seen things shared that never would have been shared even a year ago. And I have seen people who were not team players moved on to other positions. So we are making progress in this arena.

I just want to say that human nature being what it is, bureaucracies being what they are, the valves and pumps being what it is, we need to constantly be on guard with this. But let's suppose that we are. Let's suppose that we slowly migrate toward this two-by-two matrix that I'm talking about. How do we do that?

There is an old adage in business school which says that you cannot manage what you cannot measure. To what degree do we really measure in the supply chain sense the flow of information from tasking to collection and access to all of its processing discrimination and usage? There is some of that that goes on, but we will not be able to do this two by two until we can measure every cell.

How do you measure hording? Well, if I'm responsible for collecting something and I collect it and it just sits there on a disk in my control, the system can know that. Now, there may be very good reasons for that, but at least the system can know that. I think this business of smart data that knows

where it is and can kind of send out little heartbeats – say, here I am; here I am; I haven' been share yet. Here I am; here I am; here I am – (laughter) – you know, that kind of thing can help.

I think more important, however, is intrinsic motivation. And this is something that you don't hear talked about very much. And I think actually it's far more important. You know the Gallup Organization has a whole service that they offer organizations in which they come in and they say what tasks have to be done to transform an organization, and who has the temperament and the talent to do that. And the very simple approach they take is, from a management point of view, let's map the talent to the task.

And so it raises an interesting question. In our organizations, everybody is responsible for information sharing up to a point, but there are some people who have way more influence on what gets shared than others. And the question you have to ask yourself is, what is the natural temperament of those people? Are those people who are open to sharing, who believe in need to share versus need to know? Are those people who are "intrinsic rewards are sharing" or "intrinsic rewards are knowledge is power"?

You know, one deep question we have to ponder is whether these gate-keeping type positions are natural attractants for certain kinds of individuals who get certain intrinsic rewards from doing certain things. And if it isn't just a passive problem that has emerged, it's an actual emergent sociological phenomenon, where the very people who need to be the most open to sharing may attract – those positions may attract a certain kind of person. And so we have to look at that very carefully.

And so what I show here in this picture, which is very hard to see, is a bunch of people all standing on these two kind of struts where they all have to walk together. No one moves unless everybody moves in the same direction.

Some people naturally are very good at that and want to do it, and some people don't. And what I would say is we have to start thinking about our human capital versus our IT capital in this way. We have to ask: Who are those gatekeepers, and what temperament? Skills are important, but temperament is probably more important.

And when I say "de-recruit," I don't necessarily fire these sumo wrestler competitive types here. What I mean is map talent to task. There are plenty of jobs within the intelligence community and elsewhere where intrinsic sharing is not a requirement for success, or at least it's not that important. So it's really mapping temperament to task.

And I think too that a lot of you in this room are leaders, and I do not want to understate the importance of inspiration, because that's the job of leadership. And it's not about logically persuading people. It's about talking to people's hearts instead of their minds. It's like you do not manage troops into battle; you lead them into battle. And this is a battle, and you that are leaders are going to need to do this leadership, and you're going to need to lead by example. You need to ask all of yourself: Have you moved out of your comfort zone?

If you are very comfortable in the sharing that you do today, it's almost guaranteed that you're not doing it right. Because what we are comfortable with is what has always been. We have to be

uncomfortable to a certain degree. We have to do things that do not feel familiar, and we have to do it and demonstrate to our people that we are doing it. And when we see it, we have to reward it, and when we see the opposite, we have to do the opposite of rewarding it. That's leadership – not by what you say alone, but by what you do.

There is another aspect – and again, I'm going to come back to my human factors – that has to do with intrinsic motivation. You can have somebody who wants to share or wants to go and look at someone else's data.

And I'll give you a good example of this. At NSA there is this habit in analysts of only looking at highly classified information on highly classified networks. When I used to come back from Iraq, having looked at just vanilla secret stuff, let alone the coalition stuff which was regarded as basically open-sourced by the people at NSA, I would say, my god, there's a treasure trove of stuff not on the intel but on SIGACTS. You know, SIGACTS, which is Significant Activity database, records from a military operations point of view everything that happened. It has huge significance for the SIGINT business. But the analysts there weren't in the habit of doing it. I would take it and show it to them. I'd say, look, look! (Laughter.) And they were very busy. They're not bad people. They were just extremely busy, and it was not comfortable and familiar to them to look at this non-intel, non-top-secret stuff. It was not easy. It was not simple. It was not in their comfort zone.

And my point is that for intrinsic motivation to take hold, it has to be perceived to be simple, perceived to be in the comfort zone. The fact of the matter is it doesn't actually have to be there, but it has to be perceived to be there.

And I'll give you an example. I interviewed over a three-week period analysts in Baghdad when I was out there. And that was very difficult, by the way. I used the ethologists' technique. This is a type of psychology that has to do with observing organisms in their natural habitat without disturbing them. So these organisms were MI analysts in Baghdad. So I put on a uniform and I sat there at the terminal and did what they did, and I wrote reports and, you know, did stuff like that. And I would hang out in the laundry room and I would hijack them on their way to the chow hall or even the latrine because I didn't want to get them out of their comfort zone, all right? They weren't used to talking to geekazoids from headquarters while they're trying to fight a war, but they did have to go to the laundry room, and that's where I got quality time.

And I would ask them, I'd say, well, what about this? What about that? Tell me your biggest frustrations – all the normal things that a psycho-ecologist does. And it was very interesting. They all said they need one thing. They need one stop, generate a query. I type in the query and I don't care whether it's SIPRNet, NIPRNet, blah, blah, blah, blah. I just want it all to come back to me, and I don't want the million-or-none problem. I don't want to get a million stupid returns or zero returns on what I care about.

So I said, okay. Well, did you know that you have a lot of single sign-on capability in federated query with Pathfinder? You got that. And they said, ahh! It's too hard. I don't have time to learn that. Well, heck, Pathfinder actually had a mode where with two or three minutes you could do 50 percent of what you needed to do. But it appeared to be complicated. It had a whole bunch of bells and whistles

and a lot of clutter and text and stuff like that. And so even though it was simple, it did not appear to be simple.

So what we did was we came up with this federated query system. We called it Oggle (sp), and the letters may have kind of looked like Google. I'm not saying – they may have been fooled into thinking it was Google. It wasn't. No copyright or trademark infringement the lawyers tell me. But the fact of the matter is, they already new how to do it. It was zero learning for them, and it appeared simple. It turned out it was not at all simple because it had features where you could say what the query term was; was it a people, a person, an event, a date and so forth. But it was – it went over instantly. We monitored the usage of it, and it went up exponentially because it was perceived to be simple, and that was key to the intrinsic motivation.

And so I say to you, that if I pull al this together as IT professionals, if that's what you're in, what all this means really is that – two things on the extrinsic and intrinsic. If you have a partner who says, I want you to do some infrastructure so that I can do sharing, before you go out and invest scarce resources to do that, I think it's important to push back and say, what is the extrinsic motivation that you have created to make this actually happen?

How many of you have gone ahead and found exactly what you were asked to do and have it be used squat? Right? Because although you've created the pathways so that people could share, people did not want to or they didn't want to use the system.

So the number one thing is, I think you have a responsibility to be a good partner and say to them, yeah, I know we're technologists and we're not supposed to get into sociology and psychology and all that, but you know, it's kind of like binary multiplication. One times one is one, one being a true bit for – want to share and one being a true bit for able to share. And one times one equals one can share. True. But zero times zero is zero. One times zero is zero, and zero times one is zero. There was only one condition. And so you're going to do the able to share bit, but you ought to hold your partners accountable for the want to share bit before you do anything, and if they give you pushback, tell them I told you to.

So I want to wrap up here. Okay. How many of you know what this is?

AUDIENCE MEMBERS: Borg.

MR. HASELTINE: Okay. (Laughter.) This is the Borg. For those of you who don't know, the Borg are a "Star Trek" creation in which in some future humans, bitware and wetwear have fused. Now, I see a lot of Bluetooth ear buds out there. You are on a slippery slope to becoming one of these. (Laughter, applause.) I mean literally. What are you doing? You're communicating with another Borg. Right? But these people share information intrinsically and extrinsically. They're designed to share information. They cannot help but share information. They are psychically linked to every other Borg.

Now, this is Star Date 2250, circa, for those of you Trekkies. I think that's about right. So that's a couple hundred years from now. So this is our future. And heck, those Bluetooths tell us that, you know, we're getting there.

And so I think that there is a certain inevitability about it because we are smart things and we do want to be connected. But there's a couple messages that I wanted to leave you with this image.

The first one is, unlike the navigational landscape that I see from my crow's nest – which is what it is. If I'm truly in a crow's nest, I see islands and I see icebergs and I see all those. Those are what they are, and I'm going to get to them in time or not. But that's really not the environment that we're facing.

Alan Kay also said the best way to predict the future is to invent it. And if you actually think about "Star Trek," do you think it's random that this phone works the way it does? Do you know why this does this? Because Captain Kirk had a communicator. That's right. That is literally why this phone works the way it does. It was envisioned on "Star Trek," and then 20 years later here it is in my hand.

So we have within our hands the ability to invent a future which is not this future that I'm showing here, but the future that I've talked about about moving that curve. The American people, the people that we are sworn to protect, are going to demand it. Another way of putting it, to quote Seven of Nine: Resistance is futile.

Thank you very much. (Applause.)

Am I supposed to take questions or just sit down? (Laughter.) I think the Statue of Liberty microphone says I'm going to take questions.

Q: Could you do a little riff on the globalization point you made and what impact the globalization of the science and technology, particularly the rapidly changing situation in China, will have on national security?

MR. HASELTINE: I think it's profound. I want to go back to the nuclear deterrence days, where there was a doctrine that says you equip yourself not against intent, but capability. We do not believe today that the Russians want to annihilate us with nuclear weapons. Fact of the matter is, the Russians could annihilate us with nuclear weapons. And so that drives a certain response on our part: that we have to be prepared against that very low-probability capability.

Let's talk about the Chinese. How is this getting to me? What could the Chinese do if they wanted to?

If you – how – most of you probably have some kind of security clearance, I would guess. If you look at the equipment that's in your office today, that's in your pocket now, that's sitting in front of you, if you're on your laptop, where was it made? Who wrote the code? Where did Centrino come from? And if it wasn't made overseas, where will it be made in 10 years? And I'm just going to ask you, if someone has the intent, the capability will be there to do whatever they want.

Jim Gossler (sp), who is some mythic figure in our business for being very creative and also to have an evil genius kind of reputation, basically assessed that a really skilled adversary who worked the supply chain type of issues could basically eat your lunch, and you would never know it.

And so I haven't answered your question directly because this is not a classified arena. But I think you can fill in the dots. I think it's profound.

And I don't want to pick on China. And you know, I'm not saying that they have the intent, but we have to keep in mind that the capability is there.

Q: In the future, how would you work with – let's say we have a partner that's a Third World that has the – only has that $2 technology because it's the only thing they've got. Are we – how are we going to work with friends, future friends and partners that have technology that is not the same as ours?

MR. HASELTINE: Well, I think that it doesn't concern me too much, because, remember, I said that I everything is going toward IP. And that was just layers one through four, let's say, right? But there is a similar standardization that goes all the way up and down the OSI stack, and the Web is a perfect example of that. The nature of smart things wanting to be connected to other smart things is that they want to speak the same language. So I have no doubt whatsoever that that $200 thing you're going to carry around is going to talk to that $2 thing that someone else carries around.

And think about it. That $2 thing is going to have a lot of brains in it.

So I really don't think that's going to be an issue. I think the dominating factor is going to be the motivation to share with someone who has that $2 thing.

Yes, sir?

Q: You were talking about how you could start to stop, you know, letting people do the hoarding and start to reward the sharing. Do you think we're going to be able to get some sort of a system where we get the services? Everyone's talking SOA this and SOA that. Well, so what, if you're not going to measure who's using what, if we could start to put services out and start to get – to benefit some of the groups that were putting successful services out, do you think you're going to get much of a chance of doing that, sir?

MR. HASELTINE: Yeah, it's going to happen. Michelle has agreed to do it with me. Right, Michelle? See, this is a little psychology. (Laughter.) I'll remind her that in front of a thousand people she nodded yes. You all saw her say yes.

No, in all seriousness, there are efforts under way already to do this, and in fact, it's already being done with great success in different parts of the community. And kind of our job is to take those embers of help and fan them into a full forest fire. And so there is good movement in that direction. Our job is to accelerate it.

So I predict that within X years, this vision of marking and measuring, doing supply chain monitoring and measuring, and so forth, it is going to happen. But we depend on – the technology isn't the issue so much, but it is. There are better technologies than others for doing this. And one of the natural questions is do we want to hijack the rights management – VRML, and so forth, all of that that's being developed by the commercial industry, the COTS, C-O-T-S or K-O-T-S kind of off-the-shelf? Probably, to some degree.

Q: Sir, I was wondering if you could draw a comparison between information assurance in government and intellectual property protection that industry faces.

MR. HASELTINE: Ha. It's a very good question. I spent the last three years at Disney working intellectual property protection issues, and I am convinced that they are identical issues conceptually; that you're basically talking about knowing where a particular piece of intellectual property is and governing its use rules.

There is a big difference, though. There is no such thing as 100 percent safe system. It just doesn't exist. It's against the laws of physics. What you always have in information assurance or protecting commercial intellectual property is how high do you raise the bar so that the cost-benefit calculation is there. My belief is that there is a big distinction between the commercial world, in which it is important to raise the bar so high to protect Mickey Mouse – which is big, that's a high thing – but it is not as high as protecting our nuclear launch codes. And so it is going to be important that we always keep in front of us the need for "special sauce," because we do not protect intellectual property with the same goal in mind as do owners of intellectual property in the commercial arena. And I think there are deep implications for how we have to continue to do our own stuff that builds upon but does not 100 percent depend upon what everybody else is doing. We need something proprietary.

The Information Assurance Research Lab at NSA has what they call the "got slice" theory. And that means it's 90 percent or 95 or 99 percent COTS, but there is an enabling piece that is a slice that is proprietary, and that makes the whole thing as if it were proprietary. And the Trusted Platform Module – Trusted Computing Module Platform concept, I think, offers a lot of opportunity for that.

So it isn't either/or. But I do think it's a very important concept that we cannot always – and I have no animosity toward Bill Gates; this is a – just a philosophical statement – that we cannot always allow Bill Gates to decide how secure our information should be.

Q: The traditional binary computing systems that we have are quickly approaching physical limits. We've looked at things like quantum computing that allow you to then have four states for processing, and you have considerably greater processing power. Any other interesting paradigms that might really change our computing models in the future?

MR. HASELTINE: Yeah. Well, first of all, when you say “quickly,” I want to go back to this – if you look at the road map for the semiconductor industry, they show Moore's law continuing for at least another 10 years. What happens then is that you start getting into the fact that you're now down to quantum levels, and you essentially do have a quantum computer when you start getting on length scales of the order of a few nanometers or a fraction of a nanometer.

But we have an existence proof for what could be beyond that limit in DNA. DNA – and this is again due to Alan Kay – he says, look, DNA is an existence proof for a nanoscale computer. Look at how fast it does IO on a nanoscale. So I think we have bionumetic (ph) models that take us well beyond 2016.

I for one think that Moore's law is going to continue or a long time because I don't think Moore's law is about technology; I think it's about business. You find, if you talk to people at Intel and other places, that the thing that drives 18 months isn't so much how long it takes to put up a new (fav ?) is how long it takes to amortize your previous product line and make your money back so that you don't have practicide for your next generation of stuff. It has more to do with business cycles than it does technology cycles.

So I think that it's also expectation. You know, the idea of – it's interesting when you think what really caused Moore's law? I don't think it was people getting smarter and smarter about PhotoLift and going to shorter and shorter wavelengths and then, you know, evanescent wave this and, you know, direct that. I think it's more about the idea that it's possible, that it ought to be possible that as we conceive, so we achieve. And I think because human beings have got it in their head that smaller is faster and cheaper, we're going to continue on that path until we get to where we have existence proofs of what can be done today, which are well beyond where we're projected in 10 years.

Q: Hi. There's been a lot of talk about sharing of data. Is there any talk going into sort of sharing of other things, like compute cycles across agencies, things like that?

MR. HASELTINE: Well, there's been talk of it. I mean, you remember at NSA, we talked about screen saver time. If you look at the amount of CPU time that's actually used doing other than moving fishes across the screen, it ain't much.

And the question is if we truly had an ability to have a little application that poked up and said, am I busy? No. Okay, I'm going to steal you to do NSA Application X. And if we're secure enough, we can be doing NSA Application X. And if we just parse that little piece of it, part of it's going to get to how much of a thin-client world do we really go to. Is it really going to be on your desktop or are you really just going to be looking at pixels, and the real brains are sitting back in some board center, like Google is going to. Right? I don't know. I suspect it will be a combination of both.

Honestly, I think that is so far off in the future. And the problem is not so much that it isn't a good idea, but imagine the code. Can you imagine what tools you would need to write a massively parallel application that ran over different timing paths with race conditions and all this? I don't think the tools are there. It's the software tools, I think, that will stop that.

Question in the back. Yeah?

Q: We all have cell phones, and they're getting better faster and even free based on your subscription. What are we doing globally to capitalize on every person being a collector, just as the Army's going to do with every soldier it sends there, with cell phones able to take high-resolution pictures, send text messages and on and on to capitalize worldwide on all the cell phone users collecting and providing terrorist information?

MR. HASELTINE: Well, I love that question because it really starts to look at what happens with technology. Technology not only makes things cheaper and better, but it demolishes previous distinctions. The distinction between the intelligence consumption package – i.e., the terminal in which I search Intelink – to the intelligence collection package.

What this gentleman is suggesting is that the very same terminal that could push information out to someone could also be a collection device because it's going to have a camera, it's going to have a microphone, it almost certainly is going to have a software-defined radio of some kind in it, and it almost certainly will be able to link up with other software-defined radios and create multistatic, mesh networks, synthetic arrays, all kinds of things are going to be possible.

So, could you have a network of cell phones be a SIGINT collector, a MASINT collector, a COM system? Absolutely. And I'm not smart enough to figure out how all that's going to happen, but again, because this is an unclassified conference, I will just say the capability will be there to do all of those things, to not only have that individual handset be a collection tool – because again, it will be collecting photons, accoustons or whatever it is that sound waves are – phonons, I don't know – and it will be doing photons.

It will be collecting all of that stuff, and it will know exactly where it is. And it will be – and it will know who's holding it, and it will be mesh-connected to everything else. And you could have distributed kind of botware in which all of these things are talking to each other and synchronized. And because they have GPS, they're going to have a common time base, and because they have a common time base, they're going to be able to take a common coherent look at the RF spectrum and other spectrums. The implications are profound. If I have millions of cell phones out there all time linked, and I can look at all of that RF all at one time and one place, it's a fascinating thing to contemplate.

So the capability will be to do some very exotic and interesting things, and I'll just have to leave it at that. And are people thinking about that? Yes, we are thinking about that.

Yes, in the back.

Q: You mentioned that we as a nation equip ourselves to defend ourselves militarily against capabilities, but how about motivation and intent on the part of terrorists and proliferants? We've seen folks like A.Q. Khan cause a lot of damage. There are a lot terrorist wannabes. Are we doing anything? And should we be doing anything in the future to address this, and perhaps figure out how to measure that and how to do a more scientific job in trying to figure out what really strong motivations on the part of our adversaries might be?

MR. HASELTINE: Well, I'm going to answer that on two levels, which is, the first to say, since I'm a geek, I have the luxury of not having to answer that question. It's out of my domain of expertise. I just know about the – our wetware and our bitware. The adversary or the rest of the world that's – people like Tom Fingar get paid to think about that, and I know that's kind of a cop-out.

But I will make an observation that builds on the earlier gentleman's comment about how platforms are going to change. If warfare today is not about owning territory but owning ideas, and if it's a war in – the battlefield is hearts and minds of a particular population, then there are profound implications for the intelligence business. Just as you want to do battle damage assessment to figure out whether the thing you've done against a particular set of atoms has worked, do you want to do measures of effectiveness in the hearts and minds arena. And to what degree can you put your finger on the pulse of what a particular population is thinking and feeling if that is the battlefield that you're fighting. And I

think that it's quite clear today that when you look on the Web and so forth, that you have a tremendous opportunity for doing that with blogs and other things, completely in the open source arena.

So I think the safe way to answer your question is that from an information technology point of view, the ability to go out there and harvest what's being said on websites and blogs, MySpace, things like that, in a completely open and up environment, is going to be there. And we are going to have the ability the ability to understand what that kind of landscape of ideas is. And that is going to be important.

And I've walked right up to the chalk line of what I can say without getting in trouble.

Yes?

Q: On the subject of extrinsic motivation and information sharing, there's probably a considerable proportion of the audience that are really believers in information sharing, but they exist in structures with the reward-and-punishment system that you talked about. Is there any consideration for establishing an ombudsman for sharing similar to critical analysis?

MR. HASELTINE: Well, we have – I think some of you heard from Ted McNamara earlier – we have a program manager for information sharing. And his job is to promote information sharing.

We also have Michelle Weslander and Dale Meyerrose, who are in very important positions, and they get rewarded for making sharing happen. And maybe they get the opposite if they aren't successful at making sharing happen.

So that's one of the very important facts that maybe has gone past people with the creation of the DNI: that our job is to do that. We have been selected because we intrinsically are people who want to promote sharing, and our rewards system rewards us for causing it to happen. So in a sense, we do have people whose specific job is to promote information sharing. But in another sense, everybody at DNI has that job. So we're all ombudsmen.

And like I say, I think we've been making some progress. We got more work to do. It's a daunting challenge ahead, but I'm optimistic.

One last question.

Q: I'm trying to see if I follow your processes in the way you've outlined it. Anyway, what we have is a policy issue, which the DNI says you will share or we will share. And from that perspective, then you got into behavioral patterns, whether or not somebody wants to share, don't – they don't want to share, and so forth and so on. So they have behavioral issues there. Then you talked about the executable – the Squeak executable. So you're saying that as time goes on, there may be a time where these executables will reside within whatever devices, whatever thing that exists, that will make their own determination outside as a behavioral issue, a person's behavioral issue, so that there will be at some point in time no need, in effect, to have a human involved in the process.

MR. HASELTINE: That's an important implication, yeah. I mean, if we think that the dumb thing has gotten smart enough, meaning the data has gotten smart enough, where it is – we trust it to

make a good decision about whether it's appropriate to let someone share, then I think we do remove the human valve from the equation to a certain degree.

Now, it's naive to think that we can go all the way there. But I do think that there are a lot of opportunities there. I absolutely do.

Q: Thank you very much.

MR. HASELTINE: And with that, thank you very much. It's – I've enjoyed it.

(Applause.)

(END)