Remarks and Q&A by the Principal Deputy Director of National Intelligence
Dr. Donald Kerr

National Counterintelligence Executive (NCIX)
Counterintelligence Symposium

Grand Hyatt Washington Hotel
Washington, DC

October 29, 2008

DR. CHERIE GEIDE (NCIX): We're ready to begin. Thank you. For our closing of our symposium today, we're very pleased to have some special honorary speakers. And at this time, I'd like to introduce the NCIX, Dr. Joel Brenner who will be introducing our last speaker.

DR. JOEL BRENNER (National Counterintelligence Executive): I'm going to introduce the man I work for this evening. And it's a pleasure to do that when the man you work for is both deeply qualified to be doing what he's doing, and a nice guy. Don Kerr's set of experience, his resume, if you will, is extraordinary.

Let me tell you just a little bit about the high points of what Dr. Kerr has done in his career. He was the director of the National Reconnaissance Office. He was the deputy director of science and technology at CIA, the assistant director at the FBI for the bureau's laboratory division, which is essentially S&T at the bureau. He was earlier in his career the deputy manager of Energy Department's Nevada's operations, which, for those of you who understand anything about the Department of Energy, Nevada operations is an important part of what they do.

He was then at Energy the deputy assistant secretary for Defense programs and then for Energy programs. He was the director of the Los Alamos National Lab, which means automatically he understands a lot about what we do. In the private sector, because he has had substantial private as well as public-sector experience, he was the corporate executive vice president and director of SAIC and the president and director of EG&G.

He's an expert in high-altitude weapons effects, nuclear test detection and analysis, weapons diagnostics, ionospheric physics, and alternative energy programs. He's a graduate of Cornell twice, or is it thrice – three times having an M.S. in microwave electronics, a Ph.D. in plasma physics and microwave electronics.

If there is anybody in the intelligence community who has a deeper or broader background in the techniques, practices, policies, mistakes, and successes of the intelligence community, honestly I don't know who it is.

Don gets really nervous when I call him a shrewd bureaucrat. He doesn't like that. So I say he's an expert civil servant and the best sort of civil servant whose knowledge of the intelligence

community and the people in it is vast and deep. He's a pleasure to work for, a pleasure to work with, and a man from whom I learn something every time I talk to him. I'm sure this afternoon is not going to be an exception. Please join me in welcoming Dr. Donald Kerr – (applause) – who is now the principal deputy director of National Intelligence. Don, thank you.

DR. DONALD M. KERR: Thank you, Joel. Thank you all for staying this late in the afternoon. I understand I'm kind of near the end of the program. And what Joel really just told you is I'm older than most of you – (applause) – because the only way you get experience is to survive your mistakes, and I've had a number of opportunities to do that over the years. I think I did my first field intelligence operation somewhere early in the '70s. That will give you a sense of what I'm talking to you about.

I wanted to talk a little, first of all, about thank you and those who work with you for what you do. I think it's important for us to have an opportunity to talk about the threats that are part of what we're all responsible for dealing with. I think it's also fair to be honest and tell you the obvious, which is, counterintelligence often is offered in the breach. We think about our new collection capabilities, we think about our new analytic capabilities. It's so exciting to think about those new platforms and findings that we often forget that we ought to be thinking about program protection at the same time. And it's something that we need to remind people of, encourage them to do it, teach them to do it well.

It's harder today in this interconnected world that we're all part of. We like to think we're networked without boundaries. I think we've all just seen in the last few weeks that globalization really has happened. We only need to watch what's gone on in the financial sector to be reminded of that.

And those who would point back at the United States and say, well, if you hadn't securitized all of those sub-prime loans, none of this would have happened around the world. Well, each morning we wake up and find out other people bought into the same things, did the same things, were driven by the same urge for high returns, and began to disregard the connection between value and risk in ways that they shouldn't have.

Now, do we know how to fix it? That I don't know. I think that's outside of the scope of the intelligence community, but it strikes me that it did teach us all something about complexity in our world. As new financial products were invented and the actual assets became more and more separated from the financial instruments that appear to represent them, we may have developed such a complex set of interconnected things that we couldn't predict the outcome. That could happen to us in other areas as well. So I think it is something for us to study and learn from.

One of the things that we're all charged with, of course, is helping to protect the lives and livelihoods of Americans, and in particular, the integrity of our information in this age of hackers, terrorists, criminals, teenagers and nation states adept and manipulating technology.

There's some quotes that are important, too, to help focus our thinking. One that's not too old was a suggestion that a satchel of explosives, a truckload of fertilizer and diesel fuel, these are all known tools; in fact, the recipes have been online for many years. And now the right command sent over a network can have the same effect as those tools that have been out in the literature for so long because we now know that in fact one can bring down power generation equipment and perhaps other things vital to our economy or our safety remotely in ways that we've never imagined before.

These ideas were first laid out in recent times by the President's Commission on Critical Infrastructure Protection back in 1997. And of course another one we should remember too, Henry Ford once said, "There's nothing new, only the history you don't know." And when you focus on computer security and cyber attacks, that's probably a place where Henry Ford is right; we don't know the history there yet.

Now, globalization has some interesting features, and one that I think is important for us as we think about counterintelligence to think about, the United States in the 20th century was really respected and grew powerful because of our industrial capability, particularly our manufacturing capability. You could argue that our success with our allies in the Second World War was largely based on that industrial capability, the fact that we could turn out an airplane a day from a factory using the same kind of workforce, same assembly line capabilities that have grown up in the automotive industry. And that's why Willow Run, for example, was so important, not because Ford was there but because in fact bombers were produced there in great quantities.

We continued to build on our industrial capabilities. And in fact, we have equipment and military capacity that's unmatched today. But in fact our economy has subtly changed over the last two decades. And where we were once a manufacturing economy, we're today in fact very much a service economy. I'm not sure what the balance is today; there's still a lot of manufacturing in the United States, but in fact an awful lot of the value added in our economy today is in services and in information that we haven't foreseen before.

It changes the game when we think about threats because we're not thinking about protecting high-value facilities in the same way we were. And in fact, you could argue some companies don't have high-value facilities and fixed assets; what they have is intellectual property.

Some of the pharmaceutical firms are probably the best example. The technology they use for mentor, centrifuges, other things, are common products; you can find them anywhere in the world. What's really distinctive about each of them of course is the intellectual property that lies behind the drugs they produce, for example. And so in fact their assets are tied up in the minds of their employees, the patents they hold, the know-how of the people who use this fairly standard set of equipment to make their products.

And so when we think of protection both in the government sector and the private sector, it's no longer enough to think about where are the boundaries. In fact, we've got to think about where is the value and how do we protect that.

It seems to me that as I often give Joel a hard time and say, well, tell me what counterintelligence really means in the 21st century, that what we need to do is think about the changes in our economy, how that's reflected in our society and how that in turn leads us to think about how to best protect the most vital assets of our country.

Have we crafted the right strategies to do that? I'd say it's work in progress. What are the most dangerous threats that we're going to face in the next three to 10 years? We're still getting a picture of that. If you had asked, for example, 12 months ago would we have had a financial crisis as we're having today, I don't think any of us in the room – well, maybe there's at least one person – would have predicted that, but I certainly wouldn't have.

And once we've laid out some of that strategic thinking, how do we mold our programs, in fact, to go execute and deliver on the responsibility that we have to the taxpayers, to the government, and to the programs that we all work on.

We need to think about, too, about past biases that still exist in our community. I think you're all aware that the office of the DNI was really created of course in response to 9/11 and the two commissions. And it was very clear when the president signed the bill a few years ago, the words he spoke were that he wanted the intelligence enterprise to operate in a unified and collaborative way. And so if there's any reason for the Office of the DNI to exist, it's in fact to make that happen.

We have, as you know, 16 strong components of the intelligence community. They come with all sorts of ages, all sorts of cultures driven in fact by the necessities that led to their creation and molded over time to deal with an evolving set of problems. This is the hundredth year for the FBI, for example. Bank robbery is not at the top of their list today. And in fact adapting to their new national security branch and the new responsibilities that come with it is in fact one of the most important things they're doing.

In fact, they're a prisoner of another part of our economy today. You're all familiar with LexisNexis. That gives lazy reporters the opportunity to, on the one hand, hear one thing, and on the other hand, compare it to what your adversary says about you. You see that in a lot of articles today. And so the FBI is still castigated as being unable to communicate with other agencies in the intelligence community, which is doing very well. But it's too focused on the criminal investigative part of the enterprise when in fact major resources are going into the terrorist fusion centers, the joint terrorist task forces and the like. And so part of our responsibility, too, is to try to understand the real state of our community and how people in it are carrying out their responsibilities.

When I think about counterintelligence, it seems to me that the first thing in any conversation is to dispel the idea that it's just another face of security. It's more than that and it's important to recognize. It's also not just about catching spies. That happens from time to time, but in fact the major losses of information and value for our government programs typically aren't from spies and typically aren't deterred from security. In fact, one of the great concerns I have is that so

much of the new capabilities that we're all going to depend on aren't any longer developed in government labs under government contract.

So it's fine to focus on government capabilities, but we also have to focus on those out there in our economy perhaps tied to university research programs, tied in some cases to large companies that take equity stakes. Or, looking into the audience I can't help but mention our own In-Q-Tel within the intelligence community, where we in fact take equity stakes in companies developing technical products that can be used for intelligence purposes. We are not writing contracts to get them to do a special project for us; we're in fact taking an equity stake to be the first user in the marketplace and be two or three years ahead of the competition in taking advantage of that.

We have a responsibility, however, to help those companies, either the ones that we take an equity stake in, or those that are just out there in the U.S. economy protect the most valuable resource they have, their ideas and the people who crate them. I think that's going to put a new face on counterintelligence over the next few years as we realize that the real value added in the U.S. economy is in fact not just within the government sector but in fact within the private sector where in fact it's supported significantly more than by government R&D investments.

People then say, well, we need new public-private entities to help us do this. Why don't we have a conference; we'll invite them. And of course company A looks around and their biggest competitor, company B, is there at the same meeting, and they just are going to open up in front of the government staff present to communicate to each other their trade secrets, their market strategies and the like. I think we have to be a little smarter than that.

And so one of the things that we might want to think about is what's the modern equivalent of what used to be done, for example, by the director of the FBI, by DCIs in the past, when they would go to a city like Boston and they would meet, perhaps, with a hundred of the leaders of companies there that were most involved in new and innovative technologies and work, some of it very sensitive because it had a national security application that was clear; some of it not. They might be medical equipment manufacturers, for example, or developers. And give them briefings and an understanding of the external world as perceived either by the FBI or by the DCI that they were now operating in.

Now, it was a subtle request on the part of the two directors to get cooperation and access to these companies. But the way to do it was viewed as giving them something that they could use as they address their competitive markets and tried to make their businesses grow. I think we have to come up with today's version of that, and whether it's sending directors out to give talks and sensitize, or whether it's done, for example, through the fusion centers, through the FBI field offices, through some of the other presence the intelligence community has, through Homeland Security, I can't guess right now what it might be. In fact, I think the challenge is to all of you to think about what these new mechanisms might be.

I am concerned, for example, as we work through this comprehensive cyber security initiative – which is a miracle in a way, the idea that at this point in an administration, we would be able to get the president to enthusiastically agree that it's an important initiative, that OMB would put it

in the budget, but most importantly, that Congress would give us something like – oh, about 86 percent of the new top line that was requested. That's a miracle at this point in time, with the ongoing conflicts that we have in Afghanistan and Iraq.

It's an important problem, and we're going to make a lot of progress protecting .mil and .gov. And we just took care of maybe 2 percent of the most important information that's out there. The rest of it's out in .com. So how do we think about that? How do we make available what we learn trying to protect .gov and .mil, to that broader set of folks who need to protect their valuable information as well?

Well, one way to go about it is incentives. I'm not thinking about tax breaks here. We've heard enough of that I think for the time being. But we might want to ask, in today's world, what directors and officers insurance buys. In the last century, if you were a member of a board of a public company, as I've been, they had DNO insurance. And that was, in fact, insurance against the possibility that a director or officer would fail in their fiduciary duty and put, if you will, corporate capital at risk.

Well, it seems today if a lot of the assets of the company are tied up in intellectual property – if you will, intellectual capital – maybe we ought to talk to the insurers and ask, do you insure against a failure to protect intellectual capital as well? And in that way, through their premiums, provide an incentive for companies, in fact, to pay attention to protecting their intellectual property, thinking about more robust ways to train and equip their people to protect information that's stored and moved electronically. We're looking for ideas of that sort.

We also need to think about what the incentives are to use inside our own intelligence community. I think the most heartbreaking thing that happens about once a week here in Washington is to see a very sensitive operation succeed and be discussed in The Washington Post the next day – totally undisciplined approach to how we should be protecting our most important successes, as well as other information.

And it further is the case that once people see it in the newspaper they somehow feel they've been given absolution. It can't be classified anymore; it's in The Washington Post. And so you begin to ask yourself, is that a counterintelligence problem? Is it a security problem? Is it a management problem? And I think – I come out first saying, it's a line-management problem; it's, in fact, how we lead our people, how we convey our expectations to them, how we instill the behaviors we want from the time they start to work with us.

And I think we've lost some of those skills along the way, partly because of the changing demographics in the community, partly because of the way people work. In some cases, they're not as close to those that might be their role models. But I think we have some catch-up to do in this area. And we need not wait many days before we'll see another good example to suggest the importance we should attach to it.

Self-discipline is another big piece of it. I'm too old to know how to talk to some of the people we're hiring today, so I sort of do it through intermediaries. But I think it is important to be sure

that the culture that they're bringing to our community is informed by some of these sorts of issues, in terms of program protection, protection of information, intellectual property. It's not just making sure they don't get into the wrong building.

So I challenge you, as professionals you are in the counterintelligence business, to think about an expanded view of what it is that comprises the work you do, that it really is not a discipline but, in fact, a component of the overall intelligence enterprise. It's something that, in fact, intelligence professionals broadly ought to share, in terms of execution and responsibility.

And we ought to find ways to make it clear how it can be best supported, not as a thing at the margin. Oh, we've got a new program. We've already let the contract. Let's call in the CI people; maybe they can give us a little help now. It's got to be designed into the programs from the start. That used to be the hallmark of, in fact, some of our most important programs. And I think it's something we should return to, even though the programs themselves have great differences today from what they used to be.

It, of course, is well known to all of you that our other major preoccupation in the near term is that next Tuesday a senator will be elected president. Now, it's also unusual that for the first time in many decades, the candidates for election don't include anyone with prior service in the White House. And it means that we're going to have a lot of work to do to explain what this intelligence community does and what each part of it contributes to the whole.

Yesterday you may have noticed, perhaps uncomfortably, that we once again had to release the top line of the National Intelligence program budget. We're going to have to explain to people what they buy for $47.5 billion dollars. Some of that's counterintelligence. And so one of the most important things we're going to have to do is explain to those taking office what it is we bring, how what we do gives them decision advantage, and how what we do safeguards some of the most important interests of the United States.

Now, one thing we have to do too is remember transitions often, some think, bring new people to government. Actually, sometimes what they do is recycle the old people. And they're even more of a challenge, because people who've been out of office for some significant period of time – just imagine, folks who left in 1980 or – sorry, 1999, 2000 period. If they were asked to describe the intelligence community that we have today, which of course in budget is more than twice as large, in terms of people is significantly larger, in terms of scope, or our problem set, very much larger. The integration of domestic and foreign intelligence is something they wouldn't have imagined. They would've been running to the ACLU immediately, worried about that.

So how do we portray in a simple, direct way in 77 days what we are, why it's important, and why they should welcome our help as they take office? So I leave you with that thought because I can't answer that question, other than prepare for the inevitable briefings, which I think will begin a week from tomorrow morning. So we all will, of course, look forward to the end of this hideously loud campaign season, but know that there's a lot of work ahead of us.

We're in a time of war. We're in a time of economic crisis, and it's our responsibility to make sure that the handover from one administration to the next is as smooth and gap-free as any of us can make it. It's too dangerous to think of doing it any other way. So, please be thinking of it, and more importantly, I'll welcome your participation in helping us make it the best transition we possibly can as we move on to transform our intelligence community. Thanks very much for your attention. (Applause.)

If anybody has a, you know, a real hard question, I'd be glad to answer it, although I can tell you I learned from a colleague at CIA a few years ago when – you know, when they start to play "stump the dummy," go dumb early. (Laughter.) But anyway, anybody have one for me? Yes, in the back.

Q: The theme today is obviously focuses – (off mike) – underlying theme has been cyber threats and the counterintelligence threats emanating from, you know, one of the big boys on the block, China. My question is why doesn't the ODNI have a mission manager in China and do they have any plans to add that in the future?

DR. KERR: We don't have a mission manager for China by that name, because it was thought some years ago that that would be suggesting to China that we saw them as an adversary. We do have, in fact, an NIO for East Asia. And he actually has the responsibilities for coordinating collection and analysis, and not surprisingly, the largest part of his account is China. Whether people in the future will change their view about what might be a politically correct title for someone with that responsibility, I can't guess. But de facto, China is an area where not only do we have mission management going on, we have significant increases as we look forward in working that as one of our hard problem sets. Yes.

Q: Your background is in science and technology. We've been hearing about how the progress of science and technology has been making counterintelligence more important because we have more to lose. And it's been making it more difficult because it gives our adversaries additional tools. Are there ways in which we can exploit science and technology to get the job done better?

DR. KERR: Well, I mean – I think one way to look at it is science and technology and developments they've enabled have in fact been at the heart of some of the great successes of our intelligence community in the past, and presently as well. It's just harder to talk about the presently part here. Will they enable counterintelligence in any particular way that's different than enabling the broader intelligence capability? I don't know. And the reason is I've never really thought about the question from the point of view of, is there specific technology that would help in the counterintelligence area?

One thing you could think about, however, is whether given a counterintelligence threat, you might change the way in which you do certain kinds of SNT and advanced development. And that's something that you could begin to engage the technical community with. For instance, as the Anthrax case information continues to come out in the press, it was inadvertent, but quite important that as people learned more about the genetic changes in the Anthrax, they were able in fact to do attribution in a better way.

So, clearly in the biomedical, biotech area, there may be tools that are inherent in what you're trying to do that also could help the CI problem. Whether that is translatable, for example, into some of the software development – is there, you know, a genetic code that you can embed in software you're developing so that you can look for changes, for piracy, and the like? I don't know; it's not something I've ever done. But it strikes me that there are things like that that get to authentication and attribution that may be very, very important for counterintelligence that we could look to the technical community to help with. But I think it's a good question and I'm an amateur on that end of it.

Any others? Yeah. I think – the red sweater. (Chuckles.)

Q: Thank you. I think we focus on many of the hard targets, the theft of secrets, the thefts of intellectual property, the thefts of industrial secrets, copyrighted material, et cetera. What about the counterintelligence threat to our political process of foreign hostile influence operations, the use of, you might say, covert action to influence our political process, whether it be money coming in overseas on the Internet to campaigns, the use of lobbyists, use of media placement operations, the kind of soft power tools that appear to me – when I pick up the Post this morning and see eight pages paid for by the Russian government. What's being done in this area of counterintelligence?

DR. KERR: To be honest, I think you've picked a good point. And by the way, the eight pages will probably be China tomorrow, because they've done their supplement, as have other countries. You might really ask the question in another way, which is, how do we prepare those who lead us to understand when they see these messages coming that they may not be news?

The United States, of course, has used covert influence itself as a tool. So we can hardly not expect that it would come back at us from time to time. And so the question is, how do you induce a healthy state of skepticism amongst those in the Congress and executive branch who are going to be subjected to this kind of information? There's nothing we can do about that. But how do they become skeptics and fact checkers and really understand that people are trying to influence them? What's K Street all about after all? (Chuckles.) It's chock full of people who want to influence our elected representatives.

So, learning to explain to people how they might think about information they receive, how they may need to do some vetting of their sources, just as we do in the intelligence community, I think, is going to be a key, because there's no way to shut it off. And, you know, there's no way to do, if you will, counter propaganda. It comes from too many directions. So I think at the end of the day it's going to be how we prepare people to live in the environment where people are trying to influence their behavior and their thinking by the messages they're delivering. I don't know any other way. Well again, thanks for your time and attention. Good luck. (Applause.)

DR. BRENNER: Thank you, Don. And on behalf of my office, Cheri Geide would like to give you a plaque as a token of our gratitude for your – not just for today but for your consistent support for counterintelligence since you've been in office. Thanks so much.

DR. GEIDE: Thank you.

(Applause.)

DR. KERR: Thank you. It's been fun.

DR. GEIDE: Thank you for your attention and your participation today. This has been, at least for me, a very interesting dialogue, lots of engagement. And I do hope that each and every one of you will take away something from today that you didn't come to the conference with – new ideas, new thoughts, and perhaps different perspectives. With that, I would like to offer each of you to be on the lookout within the coming weeks and months for some additional information from our office. We hope to have some products that are outgrowths of today's discussions that we will be sending either links to our website where we will be posting that information or even potentially some documents.

So, again, I thank you for your participation. We also encourage you to contact us if you have ideas or thoughts about next year. Make sure that you fill out the information sheet and feedback for us. We do take that to heart for next year's planning. Thanks again. Enjoy the rest of your evening, and with this setting, many of you are welcome to continue your dialogue in the venues that are offered here in Washington. Thanks.

(Applause.)

(END)