

**CARNEGIE ENDOWMENT
FOR INTERNATIONAL PEACE**

**CARNEGIE INTERNATIONAL
NONPROLIFERATION CONFERENCE**

**9:00 – 10:30 A.M.
FINDING INNOVATIVE WAYS TO DETECT AND THWART
ILLICIT NUCLEAR TRADE**

**CHAIR: STEVE COLL,
THE NEW YORKER**

**DAVID ALBRIGHT,
INSTITUTE FOR SCIENCE AND INTERNATIONAL SECURITY**

**MATTI TARVAINEN,
INTERNATIONAL ATOMIC ENERGY AGENCY**

**RALF WIRTZ,
OERLIKON LEYBOLD VACUUM**

**MONDAY, JUNE 26, 2007
RONALD REAGAN BUILDING
AND INTERNATIONAL TRADE CENTER
HORIZON ROOM
WASHINGTON, D.C.**

*Transcript by:
Federal News Service
Washington, D.C.*

STEVE COLL: Good morning. My name is Steve Coll. I'm a staff writer at the New Yorker magazine. You are at the "Finding Innovative Ways to Detect and Thwart Illicit Nuclear Trade" panel. If you wish to be elsewhere, this would be a good time to adjust. Good time to remind you also if you are carrying cell phones or beeping Blackberries, this would be a good time to switch them to vibrate or silent.

We have a terrific panel, three excellent speakers. I'll say a little bit about each of them as they deliver their prepared remarks. Just to give you an outline of our program, each of the panelists will speak for about 10 minutes or so and that should leave us plenty of time for what I hope will be a good discussion and for your questions. When we reach that portion, I'll remind you of the usual procedures. We will have a colleague who will carry a microphone around, but I just wanted to remind you at the start that we're not only on the record, we're being transcribed. So it would be particularly helpful when you ask a question, if you choose to do so, that you speak clearly into the microphone, wait for the microphone, and identify yourself in some way that the transcribers can work with.

With that, why don't we turn to our first speaker, which is going to be David Albright, who is known, I think, to many of you, president of a very significant group that he has been running for how long, David? Fifteen years. Institute for Science and International Security, which is not only an important source of ideas and analysis but also a very important source of new information, at least in the public domain on a regular basis. David is a scientist as well as an expert in proliferation policy matters and he has been studying nuclear traffic and smuggling for really the whole time I think that he's been running this institute. So we very much look forward to hearing from him.

After David we'll turn to Matti to hear the IAEA perspective and the sort of role that international organizations play with states. And then I think in a very unusual feature this morning our final panelist, Ralf Wirtz, we're going to hear directly from the private sector, from a German corporation that has lived at the intersection of gray market and white market and black market issues for a long while, and I think Ralf is going to offer both experiences and analysis that is very hard to come across in conferences of this kind, where we're usually dominated by government and think tank voices. So I very much look forward to all three of them.

David, with that, welcome to the podium.

DAVID ALBRIGHT: Thank you very much. I'm going to stay here and just kind of read from a prepared text, and I'm getting over a flu so I apologize if I start coughing. Hopefully that won't be in the transcript.

Abdul Qadir Khan was finally busted in 2004 after he'd done a great deal of damage to U.S. and international security. George Tenet described Khan as being at least as dangerous as Osama bin Laden. And we would not be that concerned about Iran's nuclear efforts if not for Khan. Iran's gas centrifuge program would likely have foundered without Khan's assistance. Khan's arrest and confession ended a career in nuclear smuggling that lasted more than 30 years. For most of this time Khan outfoxed Western intelligence agencies and governments in his efforts to secure nuclear weapons for Pakistan. His shift in the mid-1980's to supplying other developing countries with the means to make nuclear weapons remained hidden or ignored for years. Despite his arrest, shutting down the Khan network has by no means brought a halt to nuclear smuggling, even by Pakistan. A key European corporate official said that after Khan's arrest in 2004 he saw no change in the pace of Pakistan's illicit orders for its own nuclear weapons program.

Mohammad ElBaradei, many of you know, has warned that the Khan network is just the tip of the iceberg. There is no reason to believe that illicit nuclear trade and the threat it poses have diminished significantly. Ambassador Abdul Minty, who's actually speaking on another panel right now and is deputy director general of the South African Department of Foreign Affairs, has said that the Khan network operated in 30 to 40 countries, but few of these affected countries have launched any prosecutions of members of the network. Only a handful of Khan's associates were even arrested. Minty now worries that the Khan network or portions of it have reconstituted.

Illicit nuclear trade is the scourge at the heart of virtually all efforts by would-be and several de facto nuclear weapons states to build or expand their nuclear arsenals. We must fear Iran, Pakistan, and North Korea because of their successes in nuclear smuggling. What makes this smuggling so difficult to stop is that the business is so lucrative for suppliers, who rarely worry about getting caught, or if caught, about receiving severe punishments.

Despite the seriousness of illicit nuclear trade, it is receiving scant attention in the wake of the Khan network exposure. Though significant resources have been brought to address the threat of fissile material smuggling in the former Soviet Union and elsewhere, the issue of illicit trade has receded from the nonproliferation agenda. I believe that a deeper understanding of how such trade occurs and ways to thwart it are critical and should be considered on a par with fissile material production and control in achieving threat reduction objectives.

Back in the early 1970's Khan was the first to realize that the means to make nuclear weapons could be purchased piecemeal from Western suppliers. Khan understood that through reverse engineering and duplication he could build himself an entire uranium enrichment facility one piece of centrifuge at a time, instead of buying a plant in its entirety. Khan's accomplices did not come from outlaw states and were not terrorists. They were engineers, his European university chums, or ambitious businessmen out to get rich quick. Urbane and educated, they stashed millions of dollars in secret bank accounts, and in some cases handed down the family business to their

children. They also drove the business by always being on the lookout for promising new markets.

After Khan paved the way in the late 70's and early 80's, many countries followed his path. Iraq, Iran, North Korea, Brazil, India and South Africa all encountered difficulty buying complete nuclear facilities and thus systematically pursued the illicit route to acquiring high tech items for their nuclear weapons programs from Western suppliers. Always the pioneer, Khan charted a new path leading to nuclear proliferation in the 1980's. He started to sell centrifuges and nuclear weapons designs to other developing countries with nuclear ambitions, starting with Iran.

With few moral or political constraints and a touch of ideology, Khan realized that other developing countries would pay handily for sensitive nuclear technology, particularly nuclear equipment he had tested and improved upon in his own nuclear weapons efforts. He was helped in realizing this potentially lucrative market by Western company officials who had been key suppliers to Pakistan's nuclear weapons program and saw the prospect of greater profits. He eventually reached the point in the late 1990's, as most of you know, of being able to sell a turnkey gas centrifuge plant to Libya.

Khan's success can be traced to his creation of international manufacturing and smuggling operations, always seeking businessmen eager to make money and countries with weak export controls. For example, the Khan network organized the acquisition of key machine tools in Europe and their shipment to Malaysia for use in making centrifuge components, which were then exported to Dubai and Libya. Agents of the Khan network arranged for a centrifuge subcomponent to be made by an unsuspecting company in Switzerland, using raw materials from Russia or Italy that had been ordered by a trading company in Singapore. The agents then arranged for the subcomponent to be sent from Switzerland to Turkey, where other key players in the Khan network integrated it with other parts into a centrifuge component that was first sent to Dubai and then on to Libya.

The Khan network has highlighted the danger posed by transnational nuclear smuggling rings to U.S. and international security. Yet the conditions that gave rise to the Khan network and illicit nuclear trade in general have not receded. There remains a global black market in nuclear weapons technology that is larger, more dangerous, and more difficult to stop than is currently understood. Networks similar to the Khan network may already exist or may emerge in the coming years.

Some countries such as Brazil and South Africa dropped out of the illicit trade business as they disbanded their secret nuclear weapons efforts around 1990, but others continue. I've already mentioned Pakistan. Iran continues to seek items illicitly overseas for its gas centrifuge program using trading companies or phony companies that arise from a longstanding nationally directed smuggling operation. India pursues a middle way between a legal approach and a full-blown illegal operation in its effort to outfit its nuclear weapons program, particularly its gas centrifuge program, which is increasing. North Korea has long pursued items for its own nuclear program, and is suspected of acting as an intermediary in procuring key items for the nuclear programs of other states.

Concern remains that North Korea may seek to sell off its nuclear expertise, materials and equipment to others.

Nuclear smuggling has developed into a sophisticated operation over the last 30 years. Mike McConnell, director of National Intelligence, testified earlier this year the time when only a few states had access to the most dangerous technologies has been over for many years. Dual use technologies circulate easily in our globalized economy, as do the scientific personnel who design and use them.

Nuclear smuggling involves phony front companies, false declared end-users, trading companies located anywhere in the world, and a continuous search for loopholes in laws prohibiting or controlling the export of sensitive technology to other states. Such tricks of the trade help nuclear smugglers to avoid detection, maintain their flow of revenue and, not coincidentally, make the world a far more dangerous place in which to live.

Smugglers continue to corrupt seemingly incorruptible businessmen, particularly – or increasingly in developing countries where governments are unable to monitor or control their activities. Illegal businesses can be hidden inside legitimate ones, and the enormous growth of global trade provides the perfect cover to hide the black market's transactions. Khan demonstrated that it's possible for a shady network of scientists, industrialists and businessmen to sell turnkey nuclear weapons production facilities. A developing country could save years in its quest for nuclear weapons. In the future, hostile groups and failed states could buy the facilities to make nuclear explosive material and fashion a crude atomic bomb. According to Tenet, in the current market place if you have \$100 million, you can be your own nuclear power.

I'd like to now focus on several policy remedies, two of which will be further developed by Ralf and Matti. IISS under Mark Fitzpatrick, who I think I just saw, has also recently issued an excellent report which I would recommend. It provides great information and insights into the nuclear trade and many important policy prescriptions to fix the problem.

Ralf will talk about how companies are the first defense against nuclear smuggling, yet many companies are not doing enough to thwart such sales or alert authorities about suspicious trade. The ethic of greed rather than nonproliferation remains dominant in many companies. Ralf's company Leybold and Oerlikon stand in stark contrast to many such companies. In addition, governments and intelligence agencies need to cooperate more with businesses in figuring out and thwarting the elaborate strategies of smugglers to obtain nuclear and nuclear-related goods.

National prosecutions have been reluctant to work together to bring individuals to justice that are part of transnational smuggling rings. International cooperation among prosecutors and law enforcement officials is critical to investigating illicit trade, developing evidence and convicting smugglers. Yet the prosecutions of key figures in the Khan network have shown that such cooperation occurs far too infrequently.

Remarkably, illegally helping outfit a nation with nuclear weapons is not treated as a crime against humanity, even though the outcome could be the slaughter of hundreds of thousands of people in a nuclear explosion.

Another issue is that responsible countries control sensitive information differently. Highlighting this concern at ISIS, we were surprised recently at how easy it was to get in an inadvertent way sensitive gas centrifuge information out of the Indian procurement system. The information included designs and manufacturing instructions for a centrifuge rotor and bellows, which is considered a very sensitive part in Europe and the United States, where the information is far better protected than in India.

So there is a need to reach an international agreement with key countries about the exact information that needs to be kept secret and the level and type of protection this information requires. In addition, the United States and its allies should expand their efforts to retrieve sensitive information in the hands of illicit trade networks, which for the Khan network is an extremely important issue because much of that information remains undiscovered.

Because of the IAEA's investigations of Iran, Libya, and the Khan network, it has developed extensive expertise in tracking nuclear smuggling. Because of the growth of the black market, as Matti will describe, the IAEA has established an elite investigative unit. Its purpose is to develop ways to better detect black marketeers and their customers. As this effort is more fully integrated into the safeguards program of the IAEA, it can dramatically increase the chances of detecting and thwarting illicit nuclear trade while improving the ability of the IAEA to detect undeclared nuclear facilities and materials.

In conclusion, the arrest of Khan and his lieutenants should have been a call to arms. Instead, the response has been tepid and is in disarray. Ambassador Minty worries that the lack of action against members of the Khan network shows a lack of commitment to stopping the spread of nuclear weapons. Since the Khan network was exposed, a number of reforms have taken place, but these steps have not confronted the root of the problem. Illicit nuclear trade remains the well trodden path to nuclear weapons for both today's enemies and allies. Yet few are even aware that this problem exists, let alone committed to solving it. Thank you for your attention. (Applause.)

MR. COLL: We turn now to Matti Tarvainen, who is in charge of nuclear trade and technology in the department of safeguards at the International Atomic Energy Agency in Vienna, and is a long-time nuclear regulator in his native country of Finland. Matti.

MATTI TARVAINEN: Mr. Chairman, ladies and gentlemen. I would like to make a brief introduction to the nuclear trade analysis activities in the IAEA, and more specifically in one of the new elements of this activity. We call it procurement outreach to nuclear related industries. I will briefly describe what we do, how we do it, and why – how it's linked to other departmental activities in the agency. However, I will not discuss the proliferation networks themselves, or agency investigations in this area.

The background for these activities is less than four years ago when Libya's covert program was revealed and of course it got a lot of international attention, and the agency responded accordingly. The board of governors BOG requested investigations and the department of safeguards and the whole agency intensified analysis of fuel cycle, different elements of the fuel cycle. One of the activities included nuclear trade analysis and we used of course all the information sources available for us – that is, state declarations, verification activities in the field, and open and other sources.

One of the specific actions was establishing specific nuclear trade analysis unit, Nutran (ph) as it was called, at the end of 2004. It was located in the office of the head of the department of safeguards and it became the contact point for member states for sharing nuclear trade-related safeguards relevant information with the agency.

But the message was clear for the agency and all of us. The safeguards – challenges are no more only facility specific. They are not only specific to the state any more either. They are also transnational a lot in nature with non-state actors involved.

I show here in this slide the process of state evaluation. State evaluation is one of the main departmental processes in the agency department of safeguards for drawing so-called safeguards conclusions on an annual basis, conclusions that are published in the SIR, Safeguards Implementation Report. It's our annual report. The information received from member states, state declarations, is analyzed, it's evaluated on an ongoing basis, and then we verify, plan and conduct verification activities, and the results of these verification activities are also fed into the ongoing analysis process, the state evaluation process.

In addition to the state declaration of course we use other information available, that's data from open and other sources, and this is how nuclear trade-related data is fed into the process. Two of the main conclusions are mentioned on the bottom of the slide. The first one is that all declared material remains in peaceful activities and then we also tend to draw the wider conclusion when possible, that all nuclear material remains in peaceful activities. That means that there are no undeclared activities and the information received is correct and also complete. The trade analysis serves the purpose of drawing the conclusion of the completeness aspect.

First of January, 2007, the department of safeguards underwent some internal reorganization and the nuclear trade analysis unit was renamed the TTA, Trade and Technology Analysis. Its scope was extended and we were located in the new safeguards information management division. At the same time the division and the department is strengthening analysis of information, trying to make better use of the synergies and all the information we have available in the agency.

But the main objectives of the nuclear trade analysis remain the same. First, to centralize analysis of procurement networks-related information available to the agency, then we investigate and accumulate better knowledge of the known networks and try to

reveal presently unknown networks. One of the main activities is maintaining institutional memory of nuclear trade so that the information can be used also in the future for evaluation and analysis purposes. So this nuclear trade analysis is an integral part of the state evaluation process. It serves departmental needs, especially concerning the completeness verification of state declarations.

In this slide I summarize the seven main elements I believe we need for effective nuclear trade analysis in the agency. First we need the mandate. We need to be allowed to do these kind of activities. We need resources, we need people, we need funding. We need expertise, expertise that is relevant for this kind of challenges. We need work processes that are optimized for analyzing covert rate. We need an IT system and tools that are supporting the analysts in this area. We need cooperation first internally, inside the house, and then also externally with the member states. And then we need information. We're focusing on information-driven safeguards. And my main message today is related to information.

But first a few words about the mandate. The IAEA general conference in 2005 and 2006 passed a resolution, it's the same resolution both years, that clearly welcomes the efforts of the secretariat in analyzing nuclear supply and procurement related information that is shared by member states. What is important to notice here is that General Conference invites all states to cooperate with the agency in this respect. So for us this means a clear mandate. We are not only allowed to analyze covert rate but it's an obligation. We need to be ready when the member states share information with us.

Only a few words of the supporting tools we have. The data we receive is coming in different forms, with different quality and of different importance. It needs to be processed heavily sometimes. The main tool we use is so-called procurement tracking system. That was originally tailored for the Iraq verification needs by the help of member states and it later was tailored for the department of safeguards use.

This is the computer tool that allows us to store both structured and unstructured data, and it allows maintaining the institutional memory. It allows analysis by revealing links between old and new data. It allows data visualization for analysis and reporting purposes and so on. More information is available from other sources about our IT tools.

Cooperation and information are important elements for the agency to be successful in developing better understanding of proliferation networks and responding properly. The starting point here is that networks pose a new challenge. There are no real verification tools available for transnational proliferation challenges when non-state actors are involved. Safeguard system was developed for other challenges. This is a new situation. So what we can do, we rely on the voluntary support of the member states in receiving information relevant for these activities but also expertise, research and development, training, understanding best practices and so on.

Then the procurement outreach. In 2006 the department of safeguards launched a new initiative that we call procurement outreach to nuclear-related industries. It's a

mechanism for the agency to acquire suspicious procurement enquiry data from companies if so agreed with the member states. It's fully voluntary. It's based on bilateral cooperation with the states. So member states' support remains of crucial importance for the agency to address to the proliferation networks and understanding the transnational proliferation concerns at large.

Procurement outreach is based on the premise that entities they leave visible traces when they're trying to acquire nuclear-related goods and services from the open market. They are not only controlled goods related because indications can be found anywhere. Traces can be related to single- or multi-use items. Second step is that the access can be gained to such visible traces by contacting the industrial base.

We select the companies that we want to contact based on the nuclear industrial processes rather than control lists or states. Outreach is a new source of information, information that would not otherwise be available for the department of safeguards. We are interested in suspicious enquiries in this program. Suspicious enquiries are communications from potential purchasers to the companies, typically faxes, e-mails, other contact data, contacts by third parties normally. They are usually thrown away by the companies as useless contacts that will not end up in transactions, and I think companies receive a lot of contacts like this.

In these contacts the goods themselves may not be dubious. It is the whole contact, how it's done, how it's made, what are the volumes, what are the conditions, what are the end users, statements and so on. When talking to the companies we teach them and help them to understand what are dubious enquiries, and very easily they pick up – they normally understand what is a legitimate activity and what is not.

What we ask. We ask to have the full original document or copies of them so that we can extract relevant details, store, and analyze them. So suspicious enquiries provide valuable data for us to understand who's interested in what, and to be able to respond now because safeguards traditionally verifies what already happened in the past. So this is a complementary mechanism. It's an outreach for nuclear trade analysis, to obtain unique information from diverse, primary sources of information. That is valuable because it's coming from the people who understand what these enquiries are all about.

It provides an early recognition of current and possible future covert nuclear trade activities, what goods are being sought by which suspicious organizations and so on. We're targeting intermediate traders to find both state and non-state players, so we're not targeting states. We are not interested in exports or export controlling, it's only the contact information that we are interested in. Outreach program has been introduced, now to maybe 15, 20 states. A few are already actively participating. There's more interest, several others are considering active participation, so we are moving ahead. We make progress.

As a conclusion, Mr. Chairman, I would like to say that nuclear trade and technology analysis aims at further improving the agency's possibilities to respond to

transnational proliferation risks, but we need member states support and information but also expertise, training and so on. This program outreach responds to the general conference request for all states to cooperate with the agency to strengthen safeguards. I believe that the procurement outreach is one of tomorrow solutions in curbing illicit trade. Mr. Chairman, this is what I wanted to say. (Applause.)

MR. COLL: We turn now to Ralf Wirtz, who is an executive in the export control department of Oerlikon Leybold Vacuum, a manufacturer of sensitive high technology parts that are, among many other uses, sometimes employed in the manufacture of gas centrifuge systems. Mr. Wirtz.

RALF WIRTZ: Thanks, Steve. Good morning, ladies and gentlemen. Thanks to Carnegie for the invitation. If you expect to hear another presentation about export control regulations, I hope you are deeply disappointed when you leave this conference room. It's just the opposite what I have in mind. I would like to demonstrate how we implement export controls into our company business ethics, how the company for which I work tries to actively support the goal of nonproliferation. Make you familiar with our method to detect and thwart illicit nuclear trade. And to finally ask you if this is not a recommendable and easily transferable process that other companies could follow.

A few words about the company for which I work. This is a very normal structure in these days. We have the company management, CEO, chief executive officer, CFO, and below this the operating segments. The one I'm going to talk about is highlighted here, Oerlikon Leybold Vacuum, as a single segment.

The company has a long tradition in vacuum technology. It's more than 150 years old. We have operations in all major countries in the world, a huge service network, so quite a normal business. The sectors in which we are active, we supply to customers in the semiconductor industry, customers in the research and development, in thin film coating. Vacuum products that we produce are used to coat optical lenses, to make CD's, DVD's, Blue Ray. We use it for industrial processes, for analytical and medical purposes, and for special applications like cluster coating machines.

We have also a few controlled items in the range of precision vacuum measurement. We have all the diffusion pumps, we have refrigerator-cryo pumps and frequency converters, all dual use items, but only a very few out of these are really listed. Most of them are staying below the critical thresholds.

Vacuum, I have to tell you, is a typical dual use technology. What you see here is a cross-section through a very old gas ultra-centrifuge, and on the right-hand side you see here connection to a vacuum system. I think you are all more or less familiar with these huge assemblies of gas centrifuges and cascades. And it takes many vacuum components to operate such a plant.

There is more dual use for vacuum. Missile nose cones, missile-related vacuum applications are, for example, gyro-compass manufacturing and testing, the handling of

missile propellants, space, altitude simulation of components, space components, and the coating of electro-optic devices. And finally, chemical, biological applications, you also need a single unit vacuum pump for such a freeze-drying plant in which you can produce biological warfare agents. But of course also pharmaceutical items.

A very old principle of enriching uranium was applied in this country in Los Alamos in the late 1930's, early 1940's, by means of so-called EMIS, electromagnetic isotope separation and also this process did not go without vacuum. You have here a cross-section through the vacuum chamber, and here you see the connection to vacuum pumps, very general.

The device which is described here is a so-called CALUTRON -- California cyclotron in which uranium was enriched, and here you have part of a ring magnet, which is mounted around the vacuum chamber. And this is what United Nations inspectors found in 1991 in the Iraqi desert sand. This is such a vacuum chamber of a cyclotron. And to one of these devices there was also connected such a pump, a vacuum pump. We had supplied such pumps. Our competitors had supplied such pumps. Very innocent pumps, but since then they are on the NSG controls.

This was the time for us when we said something has to happen in the company, and then new management was really embarrassed by receiving IAEA letters asking what all the company had supplied to Iraq. We established an export control department quite immediately and when we were proud of having it installed, it seems that we had overlooked something and we received a warning from a U.S. agency to practice caution regarding transaction with trading companies. And also we implemented a strict company policy which became known as the LEYBOLD charter, which mainly means very stringent voluntary self-restraint in export matters and support for the goal of non-proliferation.

But now to the trading companies. When we have concerns regarding the end use of a delivery, we simply do not supply it. And it can happen that we see this inquiry again and again and again with trading companies from many countries. Trading companies, taken for themselves, are basically welcome customers but they have to present – and I see all these inquiries. They have to present an end-use document that clearly evidences – I mean evidences. This is not a paper written by the trading company. Evidences the end-user allowing us to decide, and if we cannot decide, we transfer the case to the authorities and ask for advice.

And finally, just a number, a figure that I have to provide. Already in 2003 the amount of rejected orders and inquiries that we did not touch had reached a volume of 25 million euros. In 2003 we stopped counting because there is not much use in making statistics that nobody wants. So I say the network does still exist. We receive inquiries, and we can also confirm what analysts began to write in the late 1980's. There are typical supplier countries, mainly Western countries where high tech equipment is produced. There is typical equipment that shall be procured, for example for innocent enrichment purposes. And there's an additional observation that we made in our

company. Many of the products, many of the technologies that these customers want are much less sophisticated than you would believe when you look into an export control list. It is a fact that the end-user decides what is suitable for his purpose and what he cannot use.

Another discovery is that almost all countries qualify as diversion countries except for Latin America. I have never seen any inquiry coming from this region until now. And the final conclusion is that what many call the network seems still to be alive and kicking.

So to allow you to understand the next slides, a very short excursion into export controls. You may know that an export license is required if either the product, the technology that you wish to export is controlled. That means contained in an export control list. Or if you, the exporter, knows – this is either own awareness or awareness provided by licensing authorities – that your export has weapons of mass destruction or missile or conventional weapon end-use. You know this from discussions with your customer. You came to conclusions, you have seen drawings that allow you to come to such a conclusion, or you have received a notification from your government making your export then subject to license requirement.

But I say what the authorities get to know by doing it that way is just the top of the iceberg. The major part of the badly needed information remains in the company's archives, or goes straight into the trash. Top of the iceberg. What goes to authorities? The things which really do require a license. But what about all the rest? What about the exports which go without license, unintendedly or willfully exported without license? And what about the huge number of inquiries and projects which are not touched by industrial companies for, let's say technical reasons. You don't have the technology to supply. You can't make a quote. Or you have no export experience, you are a small engineering office. The country is far away. You don't dare to make a quotation because you are afraid to get the order. You cannot service the equipment that you deliver. Or you don't see a chance for a license. You have no production capacity because your order book is full, or you would like to deny in order not to touch it for ethical reasons. And finally, what I call the Jurassic business. The "There is something which I would like to forget deliveries," which existed also in my company. All this is lost unless we give it to those who need it, the authorities and the IAEA. We just heard from Matti Tarvainen. They need it badly for their analysis.

To detect and thwart illicit nuclear trade, we have full management support, and based on our corporate policy we work with the authorities, actively, pro-actively, on the basis of mutual trust. In all countries where we are active and observe sensitive contacts, and we do even offer sometimes vacuum technology training to interested officials who do not even know what a vacuum pump is or how it works.

We are creating win-win situations. The first winner is the authority that gains precious information for its state analysis. The second winner is the enterprise that gains trust for a mouse click. It doesn't take more to forward an inquiry to an authority.

Experience that we made is to forward interesting inquiries to the authority is really not time-consuming. And this, as I said, a mouse click to forward an e-mail with a tif, pdf attachment to an interested authority. The act of information-sharing is really greatly appreciated as quite innovative approach, and our company is finally recognized as a good global citizen.

Industry – David said this in the beginning – is the first line of fire when it comes to illicit procurement. What we supply today, remember the diffusion pumps may be hidden from United Nations inspectors for many years. Please examine if our policy is worth being rolled out.

I have a dream industry and administration united against proliferation. Thanks for your attention. (Applause.)

MR. COLL: Thank you, Ralf, very much. I'm going to – we have a full house and I'm sure many excellent questions. I'm going to take the chair's prerogative nonetheless to ask one or two. I just wanted to start with an observation, Ralf, about that terrific presentation. It begs immediately the question, how could such a model be extrapolated. And presumably one answer to the question is not immediately to pass laws requiring such conduct, since such processes are complex and not often successful. But it occurred to me that your corporation, as you tell it, adopted this approach because you were thrust into the public eye in a way that you didn't expect or wish for, and that had the potential to cost the corporation its franchise, or some portion of it. And so you responded from that position.

But in the environmental area and in other areas that we could think of, corporations have been drawn toward such modeling by campaigning, by public campaigning. It's interesting that in the nuclear proliferation area so much of the NGO community and so much campaigning is directed at states, but I'm not even aware in Germany, are there any campaigns that have come from the NGO or the public sphere, to put pressure on corporations generally to try to interpret their citizenship in some way similar to the way you've done? Has that been a part of non-proliferation campaigning in Europe in any way?

MR. WIRTZ: I have seen outreach programs from national authorities in all major countries where we are active. Officials go to companies and ask for such inquiries, so the information is available and it's not only Oerlikon Leybold contributing to non-proliferation.

MR. COLL: I guess I'm speaking more to the NGO's in that respect. So I wanted to ask one question first, which was sort of a political science question, maybe for David and for Matti, which is, do tighter proliferation export controls or reporting in your judgment actually prevent proliferation from occurring? So much of the rest of this conference is organized around the political mechanisms by which proliferation is addressed. But what is the role of actual historic – what does the historical record tell us

about the role of controls in preventing or deterring proliferation? And then what are the implications of that judgment for policy?

MR. ALBRIGHT: One of the reasons certainly that ISIS is involved in this is that we do historical evaluations, and we've often seen cases where proliferation is prevented through tightening export controls. The problem we see, and particularly we see it in the development of Pakistan's nuclear weapons program, and then the Khan network is that they were always one step ahead of the export controls. I think what Ralf pointed out is that they look at the export controls and look at what's listed, and then they buy under it. So for example, they buy valves that maybe Urenco, the enrichment consortium in Europe, wouldn't use itself, but these valves actually work quite well. They may not last as long, but they are uncontrolled and many companies are going to turn a blind eye to the end-user. They're not really required to do what Ralf's describing, which is bore into a request, since these items don't require a company to apply for an export license.

So I think you do see things stopped, but you also see a shift in the method. So it's a little like a cat and mouse game. Partly what we're trying to do, and this is why we appreciate what Ralf has been doing for years and others at Leybold. Matti has also tried to change the name of the game a little bit. And that's where I think a difference can start to have a much bigger impact. Which is, instead of focusing on export controls, you focus on export monitoring and detection. And then states can take action.

Ralf can give examples of where a trading company in China was found trying to buy things for a proliferant state. And these requests are just marvelous because the requests contain names, addresses, phone numbers. You've got all kinds of information about these people. And then the authorities can act against these people. And China, in this one case I'm thinking of, did act against those people.

So I think the idea is that the existing system of let's just improve export controls isn't working because the improvements can't keep up with the very clever proliferators. But if we add to this, these new methods that Ralf's company in particular has developed and Matti is doing and the other people are doing, then I think we can start getting a handle and thwart illicit trade better.

Now the implications for policy. I'm never quite sure what that means. But I think that one of the things that has to happen is the intelligence community, and let me focus on the United States, has to start working more cooperatively with companies. I don't know if that's a policy implication, but it's certainly a problem where the U.S. in particular is resistant to sharing information. I found it much easier to share, for example, the information we get about cases overseas. I find it easier to share it in Germany; action will happen much quicker. We were involved in stopping an export of tributyl phosphate to India. We had a walk-in that told us that India, because of actions of China to tighten its export controls against North Korea, was having trouble getting tributyl phosphate so it was trying to actually work through a German company that had an office in India. And these are long chains. A trading company in India gets a contract with the Department of Atomic Energy. They find a trading company, a German trading company

in this case. That company goes back to headquarters. That company has a subsidiary in Russia, which then approaches a Russian manufacturer of tributyl phosphate, which then sends it down to India to the original Indian trading company, which then turns it over to the Department of Atomic Energy. No end-use declarations are in any of these transactions.

We found that sending the information to Germany resulted in actions against the company. We sent the same information to the United States. We wanted to protect our source, so we took the name of our source off the faxes. The information was rejected for lack of adequate support. So I think that we've too often seen this resistance in the U.S. to help companies in a real-time way.

MR. COLL: And what is the attitude of the companies themselves by comparison?

MR. ALBRIGHT: I'm sorry?

MR. COLL: What is the attitude of companies as against governments in your experience? How unusual is –

MR. ALBRIGHT: It's mixed. I think Ralf's company is very unusual. I mean, we've worked with them for years. Mark Hibbs and I first visited Lebold in the early '90's to get a briefing from the CEO of the company. I was immensely impressed. I've worked with them ever since and they've been a model of corporate behavior. And it turns out, and I don't think we appreciated it back then, just how powerful this information is that they literally just throw away. And I think Ralf has played an important role in showing that really valuable information is in these inquiries. What he said about just clicking a mouse to send it on. It is very useful advice.

But I don't see that happening in many companies. This is partly why, again, ISIS is involved. We like to see it. We'd love to see it. We don't launch public campaigns but certainly we'd love to see a public campaign to draw in more companies to be good citizens and cooperate in stopping this insidious business.

MR. TARVANEN: Yes, I guess the question was then, do tighter export control actually prevent proliferation. I think at least two aspects, that export controls are developing then the existing loopholes in the systems are filled. I think that's preventing the semi-legal exports. Even not – that are not maybe literally denied but just filling their loopholes. But if export controls are wider applied, of course it will change the rules. I think it's like any organized crime, that wherever the controls are high, you try to find an area where your possibility to be caught is lower.

I think I would like to see the problem on a global perspective, that it would be important to have the export control at least on the minimum level in all states involved. And I think that 1540 is a good example to the steps to the right direction.

MR. COLL: Thank you. Just one very quick question before we turn to the audience, and maybe this is for you, Ralf. David as well. Several of you, I think, made reference to the rise and concern about non-state actors in procurement networks, and to some extent the Khan network was a non-state entity acting on behalf of states. There's also of course concern about non-state networks acting on behalf of non-state organizations. So my question is, are there particular signatures or issues that are relevant to non-state actors that are not present in the systems that are designed to monitor and control exports by state proliferators?

MR. WIRTZ: Steve, I cannot really say who is behind the inquiry that we receive, if it is state actors or non-state actors. It's mainly trading companies. What I can just tell you is that you often see inquiries that you get 20, 25 times through various trading companies in different countries, and it's just a specification that you recognize that you can identify. And the type of good that they want makes relatively clear what the end-user is, but normally you are not receiving it for the first time from a state actor and then from trading companies. The end users never show up.

MR. ALBRIGHT: Let me just add, I think as a future concern, particularly as the information about centrifuges permeates itself through this black network, is it possible that someone could organize the purchase of a small centrifuge plant in a quasi-failed state? I think it's a concern. I don't know how to judge the actual level of threat. But centrifuge technology, particularly as evidenced in what was found in the Khan network, is so complete in terms of the designs, instructions how to make things. Even in some cases is where to buy things. It's replicable. And so the program in the state, failed state or quasi-failed state, would need scientists and engineers, but the number needed unfortunately may be coming down as this information is further developed in the black market.

MR. COLL: Thank you. We turn to the audience now. My colleague is in the very back with a microphone and I'm sure we have many questions. I'm going to start on the left and go to the right and back and forth. Starting with the gentleman next to the microphone. I remind you please to identify yourself and limit yourself to questions. Thank you.

Q: Hi. Matthew Bunn from Harvard University. Question I guess partly for Matti and partly for David. Matti is collecting all this information from a lot of different companies in a lot of different countries, whereas any given national authority is only collecting it maybe from the companies in its country. But you're using it largely to support safeguards at the IAEA. And it seems to me it also ought to be used to help break up these illicit trafficking networks, and maybe advise countries on improved export controls or improved measures to educate their companies about what kinds of inquiries to be looking into.

And I wonder whether there are mechanisms in place to use the information for those additional purposes, or whether it's at the moment just used to strengthen safeguards.

MR. TARVAINEN: Yes, the purpose of collecting the information is to support the agency verification activities. That's a mandate we have. Of course, our experience can be used to improve awareness because very often the states and their companies are not just aware what's going on. I think that improving awareness of the covert trade would be very important, and hopefully we can in the future more use this experience.

Information flow, however, is one way, as it's clearly stated by the D.G. of the IAEA, when we achieve safeguard relevant information. We don't say forward it to the other states, but it doesn't mean that we cannot cooperate and both parties can win.

MR. ALBRIGHT: If I could just add. One is that the mandate of the IAEA to do this is still a voluntary offer. What we'd like to see is it made more mandatory, and broadened, particularly, Matti, on this issue of advising companies and countries on improved export controls. Or practices of detecting illicit trade would be very helpful. So I think that the IAEA needs to have its mandate broadened because finally now what Matti's unit can do is just go to a company, and they do approach companies and ask for cooperation. They have to do it through the state, so it's a very time-consuming process, although finally the communication is from company to Matti's unit. But still, if this is made more mandatory and broadened, I think the effort would become more powerful.

Now the other thing is, Ralf pointed out if the company sends the information to the IAEA, it often sends it to its own authority, and that becomes a way around this philosophical disposition of the IAEA that everything should be a one-way.

MR. TARVAINEN: Let me make a short comment. The need to move ahead in this area, it was also related to Committee 25 recommendations made by the secretariat, but as we know, the idea didn't fly very well.

Q: Thank you. Bill Potter, Center for Nonproliferation Studies at Monterey Institute. I have two questions. The first two to Mr. Wirtz, and I thank you very much for a fascinating presentation. You suggested that Germany and your own company was embarrassed by revelations and that this led to a change in kind of the conduct of the company, which was admirable. But I wonder if you could say something about also the change in German export control laws, and particularly what I understand to be a change which held individuals within the corporations liable for transgressions by their company, and whether that change may have made a significant difference, and the extent to which that would be applicable as a deterrent in other countries which may not have followed the German model.

And my question for Matti, obviously you interact in some fashion, your organization or your unit within the IAEA interacts with the nuclear security unit, which has a related although somewhat different mission. But I'm curious the extent to which one might improve the flow of information, even within the IAEA, given the expanded activities of Anita Nilsson's (ph) shop, and I would say a more aggressive pursuit of illicit trafficking in that particular unit, and how that might be better coordinated with

your own organization. I realize this is perhaps a sensitive bureaucratic issue, but I think the problem as I see it from afar is not only the interaction between the IAEA and various companies and national governments, but also facilitating information-sharing within the organization. So I thought perhaps you might be able to comment a little bit on that. Thank you.

MR. COLL: Start with Ralf on liability.

MR. WIRTZ: Okay, then we start with the question that you want to be answered from me. You finally now make me talk about export controls, what I wanted to avoid. It was in 1991 when for the first time the German government decided to strengthen the export control regulations. There was in principle the ability for companies to ship freely to all countries unless the good was listed on export control list. And for the first time in 1991 so-called knowledge-related export control regulations were introduced. This was at that time mainly dealing with conventional weapons end-use, and in 1992 followed by another rule that was dealing with civilian nuclear end-uses in at that time 12 countries, among them India, Iran, Pakistan, also Taiwan and South Africa. But this is not really what made the transgression, as you called it, in our company.

We were in touch with the IAEA. We were confronted with pictures with serial numbers of tons of equipment that had been found by United Nations inspectors in Iraq and it was then with extreme management back-up that we made this turn-around in the company. We became suddenly aware what we had supplied. Nobody had an idea what companies organization, state organizations like ministry of industry and minerals were doing about that. So it was an easy business. You could supply a larger number of tons of whatever it was and you had no clue regarding the end-use and it was the IAEA who opened our eyes. From that very moment we felt we are responsible for what we are doing and we should look into the potential end-users of our supplies.

This was supported. The introduction of internal export controls was supported by requests from the German government that companies should do something, and this in return was driven by papers from the US. You know that because of German exporter behavior. Does that answer your question?

Q: (Off mike.)

MR. COLL: Matti?

MR. TARVAINEN: Okay, you asked about better internal coordination with nuclear security people. For the state evaluation purposes, for safeguards verification purposes, we already make use of the illicit trafficking database information that Anita and her people are collecting, and I have colleagues here who are actively involved from the same division. This is divisional cooperation of course. But nuclear security people are mostly interested in different things. They are interested in trafficking of radioactive materials while we are focusing on nuclear materials. We use information they have already for state evaluation purposes, but the information we collect from covert trade,

that's nuclear-related, it's normally safeguard's confidential in nature. It has to be protected properly and we have committed to high information security so that we can be trusted by the companies, we can be trusted by the state, that we don't disseminate sensitive information that might be harmful for them. So yes, we cooperate already and make best use of the information they have.

MR. COLL: I think I promised to go to the left. This woman there.

Q: Thank you. My name is Anne Charlotte -- (inaudible) -- and I'm from the Center for International Trade and Security at the University of Georgia. It's a very long name. But I have a question to Mr. Wirtz, and that relates to what you described in your very excellent presentation. I wonder if you could elaborate a little bit on how you as industry representative would -- how your wish list would look like. A wish list, as for Christmas. How you would spread this healthy type of information exchange between industry and government, and how you would act in a climate, or in a climate where industries are perceived as responsible actors, and how you would take that into climates where industries are perceived as just greed-driven companies, how you would reach out to smaller, medium-sized companies and how you would improve their compliance because there's where the problem lies sometimes. And how you would kind of grow that on an international basis. Thank you.

MR. WIRTZ: You mentioned a wish list. It's the first time that I think about a wish list because we are normally not the drivers of such outreach programs. We are just supporters. A spontaneous answer could be, I am willing to do similar presentations on more occasions, and I accept normally all invitations that I get. I sometimes do even take leave to be available for convincing more industry members to follow our example.

Second point on the wish list would be that we had this room here full of industry members who could actually hear what we are presenting because we need multipliers. And I think multipliers could mainly be industry members.

Point number three on my wish list would be, can you help us in multiplying this idea, taking it to companies in your research institutes, to your students, make it known.

So what is needed for the time being, we are still in the very beginning of starting this outreach with the IAEA. What we need is a stage where this idea can be spread, made known to many more people. When it comes to medium, small-scale companies, I cannot make export controls less complicated than they are. I don't see a chance to make life easier for these people. What we can try to do is set up a symposium, just leave education to companies who charge a lot of money for export controls seminars, give more people access to less expensive introductions to the laws and regulations. This is something for the academic sector, for schools, for academies, for universities.

MR. COLL: Thank you. I owe this gentleman a question, and then I'll come to Mark.

Q: David Eisenberg, British American Security Information Council. To Ralf and perhaps to Matti as well. Not to keep dwelling on export controls, but in the course of your presentation you talked about one of the criteria being necessary for a supplying company being the evidence of a legitimate end-user certificate, as of course one would expect and presume would be the case. But trusting in end-user certificates, both in this realm and even in the conventional realm for decades has not been an insurmountable obstacle. Forgeries are quite well known, bribes, et cetera.

My question is this. Using an analogy from the trade in conventional weapons, is it feasible and preferable to conceive of, in this endeavor, something like the Blue Lantern (ph) program that the U.S. government uses for spot-checking the provenance and legitimacy of end-user certificates, not just taking the word of a trading company but actually going and ferreting out the original requester. I mean, would you see that as being a good thing, and if so, what would be any potential obstacles or impediments, if any, to industry or for government to try and do that?

MR. WIRTZ: I would find it very hard to implement this into laws and regulations because it is totally against the idea of free trade to use end-user declarations or to just keep trading companies out of the business. It is one or the other's business in the world, and as I say, I see little chance. I would like to make an appeal to industry to do this on a voluntary basis in the own interests of industry. It cannot be in the interest of industrial exporters to end up in a newspaper article after all you have supplied to network members, to illicit end-users. And I think it's also the ethical aspect that makes it quite attractive that you have something that you can then probably provide to the IAEA or to your local authorities, and from there to the IAEA, or to any other control body. We are not talking just about nuclear non-proliferation. We're also just talking about missiles, we're talking about biological and chemical things. It's not just Leybold Vacuum that is producing some items. There is more to it.

There was, I think, the beginning of this year a movie in German television by a German investigative journalist, and he interviewed Henk Slebos, one of Khan's closest friends in the Netherlands. And Slebos said it takes roughly 1,000 companies to set up a nuclear project. So it's not enough to just talk to us and to convince us. I would like to convince more people to work with end-user declarations to separate the black sheep from the rest.

MR. COLL: Mark.

Q: Thank you. Mark Fitzpatrick from the International Institute for Strategic Studies. Thank you, David, for mentioning our report on nuclear black markets. I return the compliment by noting that we drew heavily on the seminal work by ISIS in this. Our report assessed the IAEA industrial outreach program as one of the most promising of tomorrow's solutions to the nuclear black market problem.

Matti, in your presentation you noted that it is today limited to 15 to 20 countries. I understand there are resource constraints both in terms of budget and personnel and the

languages in which the personnel can work. But if I'm correct, the United States is not one of the 15 to 20 countries who are involved, which is regrettable given the global outreach of American industry, particularly the foreign subsidiaries who would be on the front lines of receiving such procurement outreach by potential proliferators. And why the United States is not involved I think is an interesting policy issue to further explore here.

As I understand it, there are two reasons. One is something David alluded to, the mentality about sharing information. The United States has a reluctance to share on a one-way basis that of course is the rule that the IAEA applies. But Matti, you said there could be a way to cooperate, and I wonder if you could expand on that a little bit more, to help persuade the United States government that there is a value in it, that in some way there can be a two-way flow.

And the second reason of U.S. reluctance, as I understand it, is some skepticism about the utility of the program. In theory it would seem to be very promising, but I wonder if you can say anything about the actual successes so far. Of course you wouldn't be able to elaborate in any details, but can you tell us whether the effort has actually uncovered any current suspicious illicit activity?

MR. TARVAINEN: Thank you very much. I said that the program has been introduced to 15, 20 states and we have indeed sent letters to maybe 15 states. We always contact the state, we contact the mission in Vienna and ask them to participate and cooperate, and several states have already done so and others are considering. We see increasing interest in this activity by member states, but these processes are slow. They easily take one or two years before we can move forward to talk to the other people in the country. But I have the feeling we are on the right track.

Then you asked about the resources. It is true that we have had a little bit difficulties with resources, especially for 2007 because we have no budget. We're living from the surplus of 2006, but 2008 we will be on the regular budget. So this is not major limiting factor, but the budget is tight of course.

We have 10 people in the unit at the moment, seven professional, three support staff. What we need of course is lots of expertise. We need better coverage of all sensitive technologies. That is not the case at the moment. U.S. is not involved in the program, but U.S. has shown lots of interest and support in other ways. We have promised to the member states that we don't mention the names of the states who support us, but the member states or the companies like Leybold, we don't talk others that Leybold supports us, but they can do it. But in the case of U.S., we've been discussing for a long time how they could contribute, and I'm expecting that we can make progress in this area.

Why this is slow, I don't want to speculate at all. I think that people in the U.S. know best how to cooperate with the agency and we are just happy with all support and

cooperation with any state who can cooperate with us, and the relation we have with the U.S. of course is very good.

MR. ALBRIGHT: Could I add one thing? Maybe as an NGO I'm a little freer to speculate. I would say that – and again, I don't know what Matti's group is producing right now, although I certainly see some of the things from Leybold. You get a window into Iran's procurement efforts, and that's immensely valuable to the IAEA as it thinks about how to verify Iran's both past declarations, and also understand its future intentions and capabilities. Iran actively goes out to buy fast-acting valves. I don't think they can make them. I don't want to delve too deeply, but every P-1 centrifuge needs three of them, and so they're going out trying to buy these things. And there's other equipment that they don't make and they go out to buy. So you get an insight into that.

The other – I don't want to go into this too much either, but certainly before Matti's operation was set up at the IAEA, Olli Heinonen was extremely active in going out and searching out the past activities of the Khan network. In fact, he pioneered this effort for the IAEA. He went out and went and started talking to companies directly, Leybold, other companies, players in the Khan network, and came up with quite a bit of information from this effort that then allowed the IAEA to better look at how did Libya get what it got and whether its declaration was complete. The IAEA learned a lot about how transnational networks function. The IAEA is still pursuing things on North Korea. So I think it's immensely useful and I would hope the United States would get over its skepticism about helping companies.

If the IAEA program is improved, it can do even more as an early warning of undeclared activities, and as a way to stop those activities.

MR. TARVAINEN: Yes, one of the elements of these activities that we support the state evaluation process, but we are somehow on the background. We make use of all the information available to us, and when new information comes in, we provide the services internally to the operations division. For example, have we seen this entity before. And if so, in which context? And we can confirm information, yes, we have seen this, pay attention to this one. Or we can say that, no, this is new information. So we can use this information in many different ways, but it supports the state evaluation. That's the purpose.

MR. COLL: Time for one or two more questions. The gentleman in the back there.

Q: Thank you, sir. I'm Ahmed Sultan (ph) and I'm from Pakistan. Repeated reference of A.Q. Khan network gives an impression that the illicit nuclear trafficking started only with A.Q. Khan. I think if you read the IISS dossier a lot of the nuclear weapons states had an indigenous nuclear weapons program. Almost every country proliferated in one way or the other. And the nuclear networks are -- (inaudible). A.Q. Khan was not the boss of the network. He was working for all interests, as the other groups are working for their self-interest. And I want to make a second point.

MR. COLL: Sir, can you ask a question, please?

Q: It's just a comment, about the 15, 20 states participating in the IAEA program. Pakistan is one of those states and in the last report Pakistan was not mentioned. Not a single incident was reported from Pakistan of missing nuclear material, whereas many developed countries were mentioned in that report. Thank you.

MR. COLL: Thank you. If we have a question, then I'll turn to the woman next to the gentleman there and move forward.

Q: Good morning. Jodi Lieberman with the Senate Homeland Security Committee. My question is for Mr. Tarvainen, and that is, to what extent are you cooperating with Interpol and Europol in your activities in providing or exchanging information?

MR. TARVAINEN: I can only talk for my unit. We have been in touch with organizations like them but we don't actively share information. We have professionally met them and talked to them and what we are interested, among other things, is the approach to practices, how to analyze information that is related to covert activities because the problems are similar in other industries. We would like to learn from the practices.

I'm sure there are other people in the agency who may have their own experience in talking to these organizations, but we don't have regular contacts.

Q: I'M Gary Birch, University of Georgia Center for Trade and Security. Question for David. I think this was an excellent panel and you covered critical issues. My question is about our ability. That is, business, government, international organizations to understand these issues and take action. I'm wondering what you think, David, about what we will be discussing 10 years from now. Will we have taken the kind of actions that puts us out front, and what might be most important to do or things to happen that will make us successful in this regard?

MR. ALBRIGHT: I see problems in the future 10 years out. Solutions are a little tougher. Let me just say at ISIS our motivation is we want to try to understand illicit nuclear trade better. We think that if we understand it better then you can raise public awareness about it.

What I would personally like to see is an IAEA that's involved in this, where states are mandated to share this kind of information where there's a credible international body that can make comments and recommendations about illicit nuclear trade, like they make comments now about undeclared nuclear facilities and materials.

I would also like to see much greater awareness in companies. To me they are the front line, first line of defense, and perhaps the most important line of defense. I think

that there's a tremendous need to find a way to reach into these companies, to change their attitudes, where now you have don't-ask-don't-tell, and the export control laws more or less support that as long as it's trading companies that you're dealing with. And you don't see companies sharing information with a lot of governments.

So I would return to kind of the motivations for this panel, which is to seek to dramatically bolster the capabilities of international organizations, like the IAEA, and find a way to have companies interacting in a much more positive way. And also interacting with each other, so as the global economy grows, you're not having more and more companies that can make a profit out of the loopholes and then arm states with nuclear weapons.

So I think this is not a satisfactory answer, but it's a first attempt.

MR. COLL: It is an excellent sketch. We've reached the end of our time, and David, you've done a good job, I think, of summing up some of the themes of the panel. They seem, in addressing the conference's overarching theme of solutions, to run in two directions. One is the somewhat familiar but crucial area of information sharing between and among governments and agencies. But the other is a relatively novel area that Ralf's presence here has helped us, I think, to think about, which is the behavior of the private sector on the front lines of illicit trafficking and trade.

I would just make one last brief observation to extend on David's, which is that we know how corporations change their conduct. We know how corporations redefine their ethical compact with employees, customers, and shareholders. It is when they feel that their marketplace demands this of them. We've seen corporations do this in areas of pollution, now carbon emissions, labor practices, a thousand areas. And it is a novel but intriguing thought that proliferation could become, from groups like this one, an element of corporate citizenship through campaigning at all levels.

Anyway, it leads me to thank you for your attention and the panelists for their excellent presentations. (Applause.)

(End of session.)