CARNEGIE INTERNATIONAL NONPROLIFERATION CONFERENCE

AFTER THE KHAN NETWORK: WHAT WORKS, WHAT DOESN'T AND WHERE DO WE GO?

MODERATOR:
JOBY WARRICK,
THE WASHINGTON POST

SPEAKERS:
DAVID ALBRIGHT,
INSTITUTE FOR SCIENCE AND INTERNATIONAL SECURITY

ROLF MOWATT-LARSSEN,
HARVARD UNIVERSITY

RALF WIRTZ,
OERLIKON LEYBOLD VACUUM

TUESDAY, APRIL 7, 2009

Transcript by
Federal News Service
Washington, D.C.

JOBY WARRICK: Good morning everyone. I'm Joby Warrick with *The Washington Post*. Happy to have you all here today.

On February 6 of this year, exactly two months ago yesterday, as most of you remember, the Pakistani engineer A.Q. Khan was declared a free man after five years of a rather loose form of house arrest. Khan came out of his villa in Islamabad asking the cameras to clear his innocence once again and denounce his critics. It was a short lived freedom, as 24 hours later, he was pushed back into his cocoon by the Pakistani government, which was apparently a little embarrassed by the episode. But a point had been made and that point was that A.Q. Khan, the lead character in history's worse nuclear proliferation scandal, was unrepentant and had escaped serious punishment.

Indeed, five years after the A.Q. Khan network was exposed, you can say the same about most of the other major participants. As David and others here have noted, this was a case that had a brilliant beginning and a rather unsettled ending. In fact, as we're coming to discover, had a kind of a murky beginning, a brilliant middle, and a rather unsettled ending.

Although to breakup the ring in 2003 was a celebrated international success against nuclear proliferation, several of the biggest players have largely escaped punishment and some haven't even been compelled to reveal the full details about what they sold and to whom. As the panel members here will probably agree, we can't even be certain today that parts of the network do not still exist.

This morning we're going to hear about some of the important lessons that can be drawn from the Khan network and its takedown. And we're fortunate to have some truly extraordinary guides to help us navigate this terrain.

The panelists here are known to most of you and they're simply the best of the best. I won't consume any more of their minutes, except to make the briefest of introductions.

David Albright, to my left, as most of you know, is the president of the Institute for Science and International Security. He was the first nongovernmental IAEA inspector of the Iraqi nuclear program back in 1996. And he's done countless original assessments of nuclear stockpiles and programs around the world.

Ralf Wirtz, to my far left, spent 15 years heading export controls for Oerlikon Leybold Vacuum in Germany and has years of practical experience in the trenches discovering and preventing attempts to acquire nuclear related technology.

And finally, Rolf Mowatt-Larssen is truly in a class by himself, a career intelligence officer who was the CIA's point person on WMD and later became the director of intelligence and counterintelligence for the Department of Energy. Rolf left government only three months ago and now thinks deep thoughts at Harvard's Belfer Center for Science and International Studies.

We've asked each of the speakers to keep their remarks to about 15 minutes, after which we'll open things up for the floor and let you put your questions to these excellent panelists.

That said, I'm happy to turn the microphone over to David.

DAVID ALBRIGHT: Well, thank you very much. For the last three decades, the proven method to acquiring a wherewithal to make nuclear weapons has been illicit nuclear trade, and that reality is unlikely to change in the future unless much more is done. A.Q. Khan's associates on three continents have been the best at it. First, they acquired the capability for Pakistan and then they decided to sell it to Iran, Libya, and North Korea. But the Khan network is not the only shop in town. North Korea does it. It both buys illicitly and, as you know from recent news with Syria, it also sells the wherewithal to make nuclear weapons.

Iran buys illegally. It hasn't yet sold it, but I wouldn't be surprised if that becomes a reality in the not too distant future. India does it. Pakistan continues to do it. Israel used to do it. It's one of the interesting cases. They made a decision to stop it. Al Qaeda tried to do it in Afghanistan and it might still be doing it.

Illicit nuclear trade has caused immense harm to international security. I don't think we'd worry very much about Iran if it hadn't been for A.Q. Khan and Iran's own smuggling networks that were getting equipment out of Europe and other places. And it could have been far worse. What if Syria did operate its reactor? What if Libya did build the gas centrifuge plant and try to go for a nuclear arsenal?

And so clearly the problem is not going to go away. And I think illicit nuclear trade will do more harm before it's ever stopped. And there certainly will be more surprises.

So what I'd like to do now is just turn to the three questions that are at the heart of this panel and talk briefly about each area, and principally focus on the Khan network and the lessons from that experience, but also bringing others.

So in terms of what didn't work, I think we can agree that what didn't work were export controls. That they didn't seem to bother, or even worry, most of these participants in the Khan network. They were ensconced in places like Switzerland, Malaysia, UAE, where they just didn't feel they needed to worry about it. Malaysia has no export controls even today. UAE had none back then. Switzerland has had very poorly enforced export controls.

Another failure was traditional safeguards. This shouldn't surprise us. Traditional safeguards were defeated by Iraq in the 1980s and the IAEA launched a herculean effort to strengthen safeguards in the 1990s. But many countries didn't implement them, and who were some of those countries? Libya, Syria – the ones that figured that they could get away with it.

Another area that didn't work well were the prosecutions Joby mentioned. There have been very unsuccessful prosecutions in the A.Q. Khan case. And what I call unsuccessful, you need to create a deterrent. If you're going to spend some time in jail before your trial and that's it, if you're going to have maybe part of the money you earned illegally taken away, you can live with that. And many of these people never went to trial. So the prosecutions were not deterrents, and there were reasons for that. These are transnational crimes being tried in national court systems. And I could

talk for hours about the problems and the struggles very dedicated prosecutors went through. These prosecutors in South Africa, Germany, Switzerland, and other places were determined to get these people, but what happened? They couldn't get witnesses. The witnesses – maybe one was in Malaysia. Maybe one is in South Africa and for the Germans, maybe they – South Africans didn't want to cooperate fully. And then evidence, what are the rules of evidence.

And so you've had a major problem mounting national prosecutions for transnational crimes where the perpetrators were throughout the world.

Now, many things did work and I think that it's heartening that so much worked. The first thing is the Khan network was busted by very sophisticated, careful, intelligence operation mounted by the CIA and MI-6. And so we can feel very – I wouldn't say secure, but certainly can feel very good that the intelligence organizations learned about these people, were monitoring these people, learned that they were proliferating, and then went to bust them. And it took years, but they did bust them.

The Syrian reactor was discovered. It didn't operate. Unfortunately, can we depend on these methods for our security? And I would say we shouldn't have to. That there's certain amount of luck in these operations. There's a certain amount of "my God, thank you," at the last minute involved in these kinds of operations. Because in the end A.Q. Khan – it would have been better if he had been stopped in the 1980s or early '90s than in the early 2000s. And it certainly would have been better to have caught the reactor before significant destruction was done in Syria.

So there are very important success, but in a sense they backstop what should be the international non-proliferation regime's response to illicit nuclear trade. And that's not happening enough.

On the safeguard's side, I think the additional protocol can play a very important role in this and it did in Iran, in 2003 particularly. The very diligent IAEA inspectors found evidence that Khan was proliferating to Iran. It was – and the way they would formulate it it's more like Pakistan, but I think they understood—based on finding or getting access to the centrifuge drawings that were Dutch and that probably meant it was Khan. And so the additional protocol combined with some additional measures were very effective in reading out Iran's illicit trade. It couldn't stop it, but it could detect it, and that's very important.

Another success or what worked was aggressive private companies' internal compliance systems. I won't spend much time on that. Ralf will talk about that. Some companies or certain companies don't want their products stand up in nuclear weapons programs, particularly in regions of tension, and they will take the steps to try to create an infrastructure internally to detect those kinds of activities. I think there were several cases involving the Khan network, where Ralf's company did detect early signs of what the Khan network was up to. But it – again, these safeguards, intelligence, aggressive company actions are operating a little bit alone and there's what Ralf's company was finding was integrated more into the intelligence community or integrated more into safeguards, then there could have been some synergies there that could have led to even earlier detection.

And I think the last thing that worked is international cooperation. There is a lot of progress on that. And in fact it was an MI-6-CIA operation to bust the Khan network is a success.

Now, let me go on to some – what I view as some solutions or where do we go from here. And let me just summarize them. And I'm not going to be comprehensive, but I'll cover three: better norms and laws, better detection, and better deterrence.

And despite the failure of export controls to deal with this problem – export controls still were the foundation of the efforts to stop illicit nuclear trade. And they're highly controversial, very difficult, but underneath them is really a moral principle, a norm which is: item shouldn't end up in nuclear weapons programs. And particularly as we now increasingly talk about going to zero, that idea can be generalized. It's not just to go after Iran. It's not just to go after North Korea. They serve a purpose which is first of all to stop countries from getting nuclear weapons that don't have them, second to stop countries from improving their arsenal, and then finally in the long run, to make it illegal for anyone to shop the world looking for nuclear weapons wherewithal. And so I think that that foundation is in need of a great deal of work. Probably the first thing is that countries like Malaysia still doesn't have export control laws. Given its central role in the Khan network and in other illicit procurement schemes, that's unacceptable.

So first priority is getting everyone to have export control laws.

There is also subsets of that of what we call states of transit concern, countries like UAE that were, basically, the receiver of supplies that then were then shipped on to wherever – Pakistan, Iran, Libya—they went all over. And so there are places where essentially front companies set up shop so they can pose as legitimate buyers and then receive the items and then send them on to the true end user. And that needs a lot of work. But again, there's ways to do that and there have been successes on that in places like Singapore, Hong Kong.

The second area is better deterrence. And there it's a range of things that are needed. One is there has to be a way found to try these people that break these laws internationally. And it's – and I don't know how that's done. We're not lawyers – (inaudible) – but from the kind of the simpleton's point of view that if you're going to go out and sell the wherewithal to kill hundreds of thousands of people, whether it happens or not, and certainly we don't want it to happen, that should be a crime against humanity. There should be some universal crime that's been committed that then if that is put in place can make all these prosecutions a lot easier. It sets up frameworks for cooperation and it sets up a norm that says that it's just not right to go sell the ability to kill hundreds of thousands of people.

Intelligence plays a role in deterrence. I'm sure part of the reason the CIA talked about this operation so much is that it does create deterrence, that we may be in your bedroom as George Tenet said, or in your computers. And so intelligence operations will remain very important in all this to disrupt these networks, to take active steps. And it has to be looked at carefully and we're very active in looking at the case in Switzerland where certain things happened. And we have to balance laws versus the importance of intelligence operations. But that's an ongoing debate.

And then the last thing I'd like to cover is better detection. And I think one of the most fundamental lessons to the Khan network is that the additional protocol should be a requirement of nations, not something they volunteer to do. That it provides the tools to, at least, have a chance to try to detect these programs earlier, to be inquisitive, to get tips from governments, companies, NGOs to look for something. There were certainly indications that Libya was up to something and that none of that was investigated by the IAEA because they weren't given the ability to do it. And I think that it's very important that the additional protocol becomes the minimum of safeguards, not something that you choose to do if you feel like it. And I think there's many ways to do that by linking it to the Nuclear Suppliers Group and also other ways.

Also the safeguards should be expanded. And I'll leave that to Ralf to talk about. Are you going to mention that Ralf? Okay. I'm exploring the idea of monitoring illicit trade. And last time an IAEA speaker talked about that at this conference. And so the safeguards do need to be improved and it's about time to do that. The last time was in the early '90s. We've learned a lot since then, and there's a lot of ways to improve safeguards.

The intelligence community obviously will play a very important role and those efforts always require strengthening and refocus, particularly internationally. I'll just skip over that.

The last one is, in a way, just to introduce Ralf Wirtz is this idea of industry-government cooperation. Industry is on the front line of defense on this issue and they have a very important role to play with their governments in detecting illicit nuclear trade before there's ever a need for an export license, or before it even comes up that they have a role to play.

So let me end there and thank you very much.

RALF WIRTZ: Good morning ladies and gentlemen. Thank you for coming to our session relatively early in the morning. Some of you may not even had their morning coffee. Very special thanks in particular to Carnegie for the invitation and for making such important conferences possible.

Joby, our chairman, was kind enough to introduce me, and I would like to add that I'm in the vacuum business since 1982, starting export sales to Near, Middle, and Far East countries with increasing responsibility for countries where my company marketed its products directly to end users, but also through sales channels such as representatives and trading companies.

The products that we make have, very many, totally legitimate civilian applications in industry and research, be it vacuum coating, including solar cell production for green energy, semi-conductor devices, medical technology, analytical applications, the production of lamps, refrigerators, air conditioners, and also uranium enrichment. Very few of our products are falling under the controls of the Nuclear Suppliers Group requiring and export license when shipped to foreign countries.

Later in the 1990s, when the export control regulations were intensified in Germany, I was requested to make sure that our company is protected in both directions; firstly, against violations of the new regulations, and secondly, against illicit procurement attempts. To say it with the words of a senior IAEA official who worked in the weapons lab office country prior to joining the agency, "prior to becoming a policeman, I was a murderer."

My thoughts will center around the questions:

First, do we really live AFTER the Khan network? Are the days of the Khan network really over?

And to anticipate the answer, a clear "probably not."

Second, which pragmatic solutions do I see as a company compliance person?

With that said, let us get back to the first question, discussing the work title of this panel: Are the days of the Khan network really over?

As an employee of an industrial company, you do not have the far-reaching capabilities and means of a government agency to analyze events, access classified information, use additional data gathered by your allies, and rely on all the administrational means and tools you have in your property as a government official, which includes monitoring communication and intercepting shipments.

You also have no possibility to arrest, interrogate, and punish proliferators.

As a company employee, you do, however, have ears to listen. You have eyes to see, and a good common sense to make a judgment if a certain business transaction that somehow deviates from the standard would fall under the "you better keep your fingers off" category.

I would like to repeat a statement which I made from the same stage little bit less than two years ago during the last conference in June, 2007. Industry is in the first line of defense when it comes to illicit procurement attempts and this, ladies and gentlemen, more than ever. Let me explain that.

Illicit procurement leaves visible traces which can be identified by not only government, but first of all industry, if necessary in cooperation with a government agency. And as a matter of fact, most of the countries wanting weapons of mass destruction do have very limited resources in terms of technology, knowledge, and industrial infrastructure and they need to import, they need to buy, they need to create inquiries and make their requirements visible and detectable in the country of shipment.

Industry knew about the infant stages of the Iranian nuclear program long before the IAEA was informed and also the role of South African companies—later the main proliferators and

suppliers to the Libyan nuclear weapons program—gave reason for concern already in the mid 1990s.

The answer to the question—can companies help to build an effective early warning system through information sharing—is a clear and unambiguous yes.

In the last six months, I have seen a considerable increase of procurement attempts, which—as we are told by government authorities—are for a nuclear program. In many media, the Director General of the IAEA is quoted as saying that there was a "nuclear Wal-Mart" out there. One or the other here may be familiar with the business concept of other chain stores; if you close just a few stores, if you shut down some affiliates, the remaining ones are able to continue to operate. Even if you close the corporate headquarters, the shops may be able to survive. Or to use another allegory, assuming the arrest of Dr. Khan and several of his business partners can be described as the surgical removal of a tumor, can we be sure there are no cancer cells left?

If we are talking about the "after Khan era," this may be wishful thinking. There may long be a second or third generation network provided a network ever existed. Some analysts say there have always only been separate smaller networks with partly and/or temporarily overlapping activities or limited mutual business relationships. My wisdom is not big enough to ultimately answer this question, but considering my role of a company compliance guy it is purely academic anyway. No matter if there was a network, if it still exists, entirely or partially, my observations are: firstly, the number of procurement attempts is currently increasing considerably. Secondly, the methods are becoming increasingly smarter. Number three, the weaknesses of globalization are utilized and exploited. And I will explain this in more detail. Having said that the methods are becoming increasingly smarter, I mean that we see a change of procurement patterns, no longer exclusively through trading companies, but through fairly legitimate end users which do not raise any red flags in the companies and to all of control systems.

One example, following tips from a European government agency, a European company discovered a new strategy used by Iran to circumvent export controls; in this case, a clever scheme to obtain equipment for a centrifuge program. In early 2006, the European company received a tip from a friendly European government to be on guard from orders from Saudi Arabian companies for 15 vacuum pumping systems that would be diverted to the Middle East country. The European company did not receive any such order, but its South Korean daughter company did receive a similar inquiry from another South Korean entity, a very large engineering firm wanting to ship such items to Iran. The daughter company consulted the central export control office, which decided to refuse this order and inform the South Korean authorities. The case could be identified because trading companies and engineering firms were so-called "non-end users" as defined in the European company's customer screening system, requiring that end user verification documents are obtained prior to any shipment to such a flag purchaser.

Then several months later, the European government agency asked again to look into a recent order placed by a Chinese company. After renewing inquiries and contracts, the centralized export control office soon found that the Chinese company that ordered 15 such pumping systems, seven of which had already been delivered to the Chinese company. The Chinese company, which

is an establishment factoring company, had ordered the pumps as part of a larger order it has received to build oil purification equipment for electrical power plants. The European company did not need its government approval to supply the pumps to the Chinese customer. The sale did not require license as it was not at all suspicious. The Chinese company had not previously been associated with illicit activities.

After the discovery, company officials immediately contacted Chinese company and asked for the end user of the equipment. The Chinese company official was vague. He said that the equipments, including the pump systems, were for an overseas customer, and, in fact, they already exported the seven pumps systems, but it refused to reveal the customer. All further shipments were stopped.

The Chinese company finally demanded the rest of the pumps or all the money back. Then it cancelled the order, perhaps to prevent having to admit at some stage that its customer was Iran.

European government authorities were notified, one of which learned from the Chinese government that the pumps did indeed go to Iran. Although they did not learn the exact end user, they believed Iran's centrifuge program was the likely customer. And the story's not yet over. The European government agency believes that the requirement for the remaining items is still alive and will materialize somewhere, out there in the global market. To procure through legitimate end users which do not raise any suspicion is a procurement pattern which we begin to see much more frequently and which was not applied before.

Now, to some weaknesses of the globalization:

Another circumstance which is used during procurement missions is that many industrial companies shifted production of hi-tech commodities to low cost countries. There is a tendency to make use of the fact that many countries, although they are eager to catch up with respect to implementation of U.S. and EU level export controls, could not reach out to a larger number of domestic companies and hence the awareness of these companies is rather low. While the U.S. or EU company headquarters have mostly export control systems, they widely ignore that they should increase the defense level in their producing and exporting entities in countries which became the winners of the international cross competition and profit race.

It is in a way shocking how many trade control executives in U.S. and European company headquarters have little or no awareness of the huge loopholes in their global compliance organization. Alerted to that extent that it even, in several cases, insist that they have no responsibility at all for global compliance of their companies and that they see little chances to find qualified personnel in the respective country.

This attitude is only topped by the argument that if a country has no or only low level export controls, it should not be expected from a profit oriented industrial enterprise to be more catholic than the Pope himself and to replace lacking regulations by company standards.

This, by the way, ladies and gentlemen, is to some extent supported by the United Nations "Global Compact," a code of conduct that requests registered enterprises to adhere to 10 principles. You can learn more from the Web site www.unglobalcompact.org. Thank you. That's not yet the end. (Laughter.)

So let me go ahead. The Global Compact asked companies to embrace and support and enact, within their sphere of influence, a set of core values in the areas of human rights, labor standards, the environment, and anti-corruption. And I skip all the rest. There is not a single word about nonproliferation in this U.N. Global Compact.

What else does not work? Keyword "catch-all" controls. The core, the nucleus of the "awareness" related export control regulations is the "positive knowledge" of the exporter about a WMD or missile end use. Only a very few countries go a bit beyond this wording and impose a license requirement if the exporter has "reasons to believe" or "grounds for suspecting" that the goods he intends to export are for a WMD or missile end use.

Well, we all know that whenever a country initiates a WMD program, this does not happen necessarily openly with the international press being present at an inauguration ceremony, or kick off event, or nice Internet presence, TV spots, and glossy brochures. Rather the country will do everything it can to make sure that the programs will be camouflaged, most of the operations be steered by intelligence services, and that nothing leaks through.

Even more unlikely, that the company which because of its international professional reputation and high quality standards is targeted by clandestine programs, will be notified openly that there is an illicit end use. The company will not be shown drawings or specifications, nor any other data that would reveal the end use. Subsequently, there will hardly ever be the required "positive knowledge" that triggers an export license application, or prior to that, the management's good common sense that would prohibit to take any additional step toward such a business transaction.

With view to the nature of the covert procurement attempts, it is also unlikely that an exporter will have "reasons to believe" or "grounds for suspecting" that this export sale could be for WMD or missile end use.

Coming to the keywords "fines and sanctions." A few years after the removal of the previously mentioned tumor, none of the accused is in jail. You know who I mean. Let us try to remember. In 2003, a German vessel was intercepted on the way to Libya. On board were centrifuge parts for the country's well-hidden nuclear weapons program. After the interception, Libya hurried to go public and admitted its WMD ambitions, disclosing the names of some of the main actors as a sign of good will. We all know about the arrests of Malaysia, South Africa, and Switzerland. Dr. A.Q. Khan, who admitted that he helped a variety of countries to acquire nuclear technology, was pardoned by his head of state. Others were put in pretrial detention, but as of today, nobody is in jail. All previously arrested and accused proliferators are free men a bit more than five years after the interception of the vessel.

The key persons in South Africa did all turn state witness, with the exception of their leader who got a suspended jail term with five years probation which he spends in his luxury apartment. The German engineer—extradited to Germany by Switzerland—made a deal with the court and got a six years jail term but will, owing to his long pre-trial detention, not serve a single day. Not to forget that he had to pay a few million dollars fine, but that will not make him a poor man.

Another engineer in Switzerland claimed to have been part of a sting operation working for the CIA in Malaysia. His is today a free man, saying in a recently broadcasted TV interview that almost five years of prosecution and pre-trial detention changed his life. I have to admit that I'm deeply impressed. (Laughter.)

As long as there is no real and much more efficient deterrent, ladies and gentlemen, as long as it does not really hurt, you will know that if you have children, then the educational effect is almost zero or less than that. It even inspires and encourages to see how far you can go.

What else does not work? If you were an eager reader and followed the progress of the investigation after the Libyan nuclear weapons program was discovered, you would have to come to a similar result:

The real scandal was the lacking willingness of countries to provide information that would have allowed to support the prosecution of the above mentioned criminals. I know that the names of several of the network members were put on the U.S. Sanctioned Party List by the previous U.S. administration by means of a Presidential Order, but I apologize. This does not make me shiver.

Before I turn to the final chapter, namely the question "where do we go," let me briefly summarize some of the above points because some of them do already contain a potential solution. Firstly, inquiries with nuclear or perhaps even WMD background are increasing. Secondly, many of the actors, in particular trading companies, are still the same as during the Dr. A.Q. Khan era.

Number three, it cannot be precisely determined if we are really AFTER the Dr. A.Q. Khan era, if other networks exist, or if there are second or third generation networks. Number four, the procurement patterns have become smarter with a tendency to make purchase attempts via legitimate end users, thus much harder to detect. Number five, catch-all regulations are not really effective. Number six, the globalization offers loopholes, owing to different regulatory levels in emerging and even more advanced countries. Seven, companies should install centralized "detection hubs" for sensitive inquiries as core of their corporate compliance efforts. Number eight, fines and sanctions for proliferators should be drastically intensified, and then the international corporation, in particular, the exchange of information relevant to investigation and criminal prosecution must be considerably improved.

Finally, where do we go? I do not believe that we really have a choice. The directions are given by our good common sense. As long as countries or terrorist organizations make increasing efforts to secretly acquire nuclear technology, we are forced to react. I have little doubt that almost everyone here in this room shares this view. The motto of this conference is "Nuclear Order – Build or Break." The opposite term of "order" is "disorder" or "chaos." And insofar the question

will finally have to read as: "Nuclear order or nuclear chaos." I do not intend to waste your time waiting for your answers.

We have to stay ahead of things, controlling them. This means we need to be proactive, not only by making efforts to achieve improvements of the circumstances I criticized a few minutes ago. Learning from other countries, we can create here in the U.S. an environment in which government authorities and industrial companies cooperate with the same goal, that is to proactively build an alliance and jointly strengthen counter-proliferation efforts.

Coming back to what I said earlier, the nuclear wannabe states have requirements for technologies that need to be satisfied. The demand materializes, becomes visible in nuclear and industrial companies, which receive inquiries long before these are turned into orders and later shipments. As a member of fact, many of these inquiries will never become orders, for various reasons. I am in several compliance working groups and have regular contacts with colleagues in the export control community in Europe. Whenever I mention suspicious inquiries, there is consent from my colleagues that they also do have such requests for quotation, and that they just either file them or put them into the trash bin.

The information potential in companies is huge, the awareness exists, but in particular in USA, companies do not dare to share such information with the government authorities. Rather, this is what I'm told when I have such discussions here—do they state they have to fear suspicion, investigation, monitoring from and through government agencies.

Frankly, ladies and gentlemen, I would also keep my big mouth shut if all that I get in return for my good citizenship is problems with national authorities, where criminals like the above-mentioned proliferators walk away as free men after a while.

The question that certain government authorities here in the U.S. will have to answer is if they can really afford to continue with their policy to repel and deter their own companies, running the risk that they will never get access to precious information which companies would like to offer if only they could be sure that they will not be facing problems for having received a letter or an e-mail that they did not even want to receive at all.

Another question that does, however, have directly to do with the afore said, and this will have to be answered by the **global** counter-proliferation community, is, if the global community can afford to have an ally which willfully disregards such a wealth of information as companies can offer. It is not a joke, ladies and gentlemen. I have colleagues here in the U.S. export compliance community who envy me because I can talk freely and without a trace of fear with European government authorities about certain inquiries that we receive. In several countries, government agencies are very happy if we facilitate their responsive work, and the return they warn our companies if they think they know something that could help the company to then turn down certain requirements.

Can the U.S. administration afford to dominate—because this is what I'm told it does—its exporting community with an iron fist, or is there a chance that we change from a hostile

environment to a respectful, or even amicable, industry-government partnership to help secure the nuclear order? Don't we all have the same goal and answer when the question that comes on the table is: "Do we want a second Libya, more Irans and North Koreas or perhaps a nuclear power named al Qaeda?"

You may have heard that there is an initiative in the U.S. named C-TPAT, the Customs-Trade Partnership against Terrorism. The initiative is led by the Department of Homeland Security. Companies need to make sure that nothing that could be of potential danger reaches the U.S. via the supply chain. Many companies have registered as C-TPAT members certainly because of the minor incentives which the program offers, but most of the approximately 12,000 registered member companies have just joined because they thought they should do so as good citizens who just would want to earn their money in peace.

I'm not aware of any such alliance for the purpose of counter-proliferation. You will know the answer to the question if that's a shame or not.

Finally, working with the IAEA. Since a couple of years, an increasing number of states have a cooperation with the IAEA. An established unit in the Department of Safeguards analyzes data obtained from member states, which agreed to share information with the IAEA, in full accordance with the United Nations Security Council Regulation 1540. This resolution requires all states to establish export controls needed for targeting, especially in non-state actors. It does not require states to share data with the IAEA, but allows, of course, to do so if states are willing. The IAEA general conference has endorsed in its resolutions since 2005 these trade analysis activities and has invited all states to support the activities of the IAEA Secretariat.

And just for the full knowledge, support, and participation of the member states that a few companies, each in these member states, do already contribute to the state evaluation process and the institutional memory of the International Atomic Energy Agency.

It is desirable that many more states—and their companies—give a commitment to fully support the IAEA and comply with its requests to share possibly sensitive inquiries. The inquiries are encrypted when passed on, and the data stored and evaluated by a few staff members only who have special authorization. The offices are secure areas with keypad activated alarm and anti-analysis units. Computer network itself is strictly separated from the general network that the IAEA maintains, including the mailing system. The fact that the 'Trade and Technology Analysis Unit" is part of the much larger IT division within the Department of Safeguards warrants the highest level of confidentiality and professionalism.

While this program is already underway, it should be considered to establish similar analysis units for non-nuclear weapons and missiles in other organizations under the umbrella of the United Nations or the nonproliferation regimes to name the Australia Group and the MTCR.

Again, ladies and gentlemen, the question "where do we go" is purely academic, at least in my opinion. We cannot let proliferators go ahead, knowing more countries may have weapons too dangerous to name in just a few years. As I said, the directions are given by others and we are not

even allowed to decide about the speed at which we want to progress. If you want to decide about direction and speed, you have to be on top of everything, controlling it with the ability to stop it when and how you want.

Looking at the recent development in several countries, I do not believe that we are controlling these processes. And to return to the previous allegory, we do not only need good surgeons, but also oncologists and other experts which are all available and just need to be made part of a medical emergency team because the global security has ended up in an intensive care unit.

Unless and until we have a dialogue with the known and potential wannabe countries, at a reasonable level and on the basis of mutual trust, I see no other option but to enhance the methods of counter-proliferation through information sharing with industry and other mentioned tools and solutions and to increase the speed.

I hope I did not bore with my thoughts and I hope that that could contribute to another badly needed stimulus package. Thank you for your attention.

(Laughter, applause.)

ROLF MOWATT-LARSSEN: What I'd like to try to do here is outline some ideas that could become the basis for some give and take. And I think some of them are self explanatory. Fortunately, we've heard a lot already from my colleagues, and I'll, in fact, try to cover some new ground. And I'd like to start with, I think, what's an under current felt in this session, as well as throughout the Carnegie conference here, which is the intelligence role. And I might just very briefly liken it to a stream where at the source you have, of course, the security of materials, of things that protect technologies and secrets.

At the midstream you have – of the efforts, some of which we've heard today, monitoring, safeguards. And then when all that's essentially failed, you've got the intelligence downstream that's supposed to pick up what's gotten through. And then that of course becomes the really critical vulnerability because that assumes that once it gets through, particularly in the age we live in now, there's an increased likelihood that all that nuclear technology and/or materials will end up in the hands of someone who will use it. And I think that's what's fundamentally changed the threat and I thought President Obama's speech yesterday in Prague really drives that point home. That we simply can't think of these problems as we have in the past.

And that's really my theme for the comments I'll try to make here, is that if you think the way we have thought about this, whether we're talking arms control, but certainly in the world of intelligence action and implication of the A.Q. Khan, both in assessing the things we're doing to stop networks like that from occurring, as well as the ways that we need to find and neutralize networks like this in the future, we are going to fail.

So that of course, if you're going to be serious about that, means that you've got to come up with what some might call provocative new ideas. And as I offer a few here, I don't even know

myself whether those are the better ideas or those are the ones that would stand the scrutiny that I hope they'll receive. But my point in putting them out here is to in fact make people think about it.

This slide really just speaks to the exceptionalism. I want people to understand, and it's not to praise the intelligence community here in any way, that what happened with the A.Q. Khan network was an exception. And it raises a question for the intelligence professionals around the world, not just the United States, about whether we can count on them to stop every threat every time we see it happen.

These are some of the intangibles. And you see a lot of talk about creativity, innovation, resources not being enough. We have a tendency, particularly in the United States, to think if we put enough money into a problem it will be solved. In fact, I would say, we have to think our way through many of these problems. The essence, I believe, of terrorists and others who would go nuclear is the desire to pull us down at their level, make it a man on man battle, in which they think they can prevail with ideas, innovation.

Think about 9/11. It could offend some crowds to say it was one of the most elegant operations I've ever seen as an intelligence officer.

The other thing I think this slide raises in terms of imagination is thinking through new ways. And I just left IAEA in Vienna last week, suggesting, which was picked up by Reuters, that IAEA might, in fact, need an intelligence arm. And I'm not here today to flesh that idea out. My idea was a very thoughtful suggestion that I think warrants further consideration. If we're serious about multilateralism, if we're serious about trying to improve the IAEA's efforts on other sides, the go it alone model, which is essential what we had, is froth with a lot of peril. I've been on the A.Q. Khan rollercoaster and the al Qaeda nuclear terrorism rollercoaster and it's a harrowing ride. As David referred to, you get there at the end and you're just happy you got there. But think how late in the process we caught the A.Q. Khan, the Libya program, the attack on the Syrian facility, et cetera.

In particular on the finishing a job aspect, we've hit some of that. The notion that you can have the Pakistani bomb designs on a computer of a European supplier somewhere and push a button and send it anywhere is something we have to live with forever. I don't think we'll know where that material can be – a disk that could be passed to the Iranians that will, say, overcome the problems they've had with enriching to highly enriched standards. Those are obvious implications of the A.Q. Khan network. Whether it's over as a network or not, you have that prospect of running into intelligence challenges in the future.

I would add that particularly the scare we had after 9/11 as you recall in timing was until 2003 we really dealt with the Libya program and A.Q. Khan network publicly. But even in 2001, obviously, we knew. So when I was called back over to CIA to head up the terrorist weapons of mass destruction effort, I spent once a week hours with the A.Q. Khan people to compare notes. Our worst nightmare was that al Qaeda has somehow managed to leverage the A.Q. Khan capabilities, if you can imagine. That is the specter of what we're dealing with in this century, a sophisticated effort like in – and by the way, we hope the answer to that is it didn't occur. That's the

best answer we have at this time. But we did have the scare with the Pakistan NGO and in fact that group we believe we nipped in the bud. It would probably have been in the early years of A.Q. Khan if you want to make an analogy of looking at that.

I think what it all boiled down – I tried one slide to offer thought here and I won't go explain it in any detail. If you take a look at it, all it really suggests is that the way that nuclear threats have changed fundamentally is that the possibilities of a pathway to a single bomb, as President Obama said, "if a single bomb, going off in a city somewhere in the world is a threshold, the pathways to a single bomb are entirely different and far more – far greater in terms of numbers of possibilities than of a state developing a weapons program in a state to state context." And you've got all these examples of states working with states, groups in states, groups with groups already.

And of course, I would say those pathways can be enabled by shortcuts, and, essentially, I would look at networks as shortcuts to the bomb. There are ways that enable. Now, I'm putting this up here for you to look at, but I won't go through it. Again, I just want to put it up here to tee up a discussion. It's not just the nuclear supplier networks we're looking at. Again, it is not a state program, particularly if a terrorist group or a sub-state actor wants to achieve a nuclear – one nuclear bomb capability. It could be facilitated through a number of other efforts and aspects of the effort can be facilitated, everything through terrorist financial networks. We've seen in trafficking of nuclear materials the role of organized crime. We saw in Abu Musab al-Zarqawi's network, which was working with chemical biological materials. We saw a heavy people smuggling emphasis as a way to get people in and out of Europe. We've already seen the importance of trusted brokers working with terrorist groups, people on the inside. Insider threats we were calling on the nuclear security world. We have seen insider threat related phenomena as possibly presenting shortcuts for terrorist groups.

I'd submit all of this to really this test, particularly in terms of looking at the nuclear terrorism threat, which is simply that if you don't have materials, you can't make any bomb to go off in any city. And so a really important litmus test, if not the decisive Armageddon test, I would say, is our ability to assure ourselves that there are no materials in sufficient quantity available on the black market that any group or state can achieve. And if you look at the record on that, and I think we have to be very harsh in our standard, the standard is enough material for a single bomb. Once again, the record doesn't look good. You have 18-19 incidents as publicly recorded by the IAEA and others of weapons usable materials since 1993 that have been seized on the black market. You have a – in none of those cases, as I recall, was the theft reported from the facility of origin, which is very worrisome. You have materials that are unrecovered reportedly from several of those cases in significant quantity.

All those cases, to my knowledge, were serendipitous. They were not the result, as in the case of the A.Q. Khan network, of going out, looking for it, and I would add that when the A.Q. Khan intelligence effort, and obviously I can't get into great detail here on that, started, it was not directed at A.Q. Khan or even the Pakistan program. And so the idea that we can go out and proactively hunt for materials is something that's not yet reached critical mass in the world's intelligence organizations. And this, in a sense, by – as those of you have seen many of the things I've said over the years, this is my most important message, is until we get to a point where there

simply is not weapons usable material on the market, there are no seizures of that material, we cannot say we're succeeding. Until we can stand in front of people and say we've recovered and resolved all the cases of nuclear materials from the past that may be missing, we have to say that we've got a problem. And in particular, since in the current model we've got an under-reporting of material that tends to stem from obvious self interests of the nations involved, a suspicion, mutual mistrust that comes from having been stung on occasion, which has occurred, and not coordinating.

This is the reason essentially that I called last week in Reuters for the IAEA to have some form of intelligence, not only to conduct its work, but as a rallying point where countries can at least consider what is possible to share in a much broader scope than on a pure go it alone basis.

There were two others, I would call shortcuts, enablers, or points of concern which A.Q. Khan really sheds light on. The first of those is, of course, the possibility that future networks we'll have to monitor, in addition to those that I've showed on my previous slide, might include aspects of the proliferation risk of nuclear energy. Now, I'm not standing up here to say that nuclear energy is a problem or we don't need – in fact, I believe we do need increased nuclear energy globally and it's already a reality. But as that occurs, as there are more materials available in more places, being moved and stored with reprocessing is still a reality in the world.

This has greatly complicated the permutations of the problem, the likelihood that a pathway could be successful involving those materials, where historically, at least in the last 15 years, the emphasis on – at least as we look at smuggling databases and what has been done on what we would call highly enriched or highly enriched uranium, plutonium, and now we've got to really be thinking also about products of the fuel cycle. We have, but not much and it certainly hasn't gone deeply into the cultures of the responders, whether we're talking law enforcement, intelligence or for that matter even customs types around the world.

The other problem is the increasing availability of nuclear information on the Internet. And what that does is create a potential shortcut combined with the cooperation, the various possibilities of groups working with groups in this regard, and particularly with more sophisticated tools to aggregate data, in other words, knowledge based networks, knowledge based on what's needed to produce a bomb, in terms of material, is increasing.

And that is why I would in conclusion sum up the problem by saying essentially what we're talking about, I believe what the president so skillfully laid out in his speech was a new paradigm which has now created a great urgency in what we're trying to do, a much more comprehensive basis and a time urgent basis, which is simply that states are seeking the powers of groups. It's not just with nuclear terrorism. It's with biological. It's with cyber. It's with the powers of state transferred to the individuals. And as long as we've got extremism in the world and groups like al Qaeda that have declared their intent to use those tools, we're at a much graver risk. And A.Q. Khan essentially was, I believe, the single most important light that's shining on ways that we need to attack this problem and new approaches in order to do it more effectively than we have in the past.

Thank you.

WARRICK: Let's thank our panel.

(Applause.)

We have just over 30 minutes for questions. Rather than have you stand up, you just raise your hand if you have a question. We'll get a microphone over to you. We'd like you to please state your name and your affiliation. And please, as we have a limited amount of time, please try to keep your questions brief and specific to members of the panel.

And while you're thinking over questions, I just have a quick one to open up the entire panel. I'd just like for the panelists to address the issue of the importance of state support for these proliferation networks. I'm wondering can these networks truly exist without state support. And that's a question that's relevant as we think about the history of the Khan network and its relationship with Pakistan, but also as we assess the potential for non-state groups to acquire significant weapons programs through these networks and – sure.

ALBRIGHT: Yes, I think the state support originally is vital. Khan would have been nothing without Khan Research Laboratories and that gave him everything he needed to proliferate. But unfortunately, it can happen without that kind of state support and I think with terrorists that may actually be how it takes place, where they'll be picking up what they need without any state involvement. I want to emphasize North Korea. We don't know how North Korea helped Syria. And I say "we" in a general sense. We get no reports from the intelligence community, from states, IAEA how did North Korea provide the wherewithal to Syria to build that reactor. It's not a sophisticated reactor, but still you have to get graphite. You have to get various reactor components. And as far as I can tell, that's a big mystery and that's very unsettling because North Korea was obviously running some kind of network to acquire things overseas, to supply things from North Korea and would always known about it. And, as far as I know, North Korea's continuing despite its commitment in the Six-Party Talks process, the Singapore Agreement.

So you have a country there that is – a state that's actually proliferating and therefore could pose a severe risk in the future if it decides to sell a nuclear reactor to someone else.

MOWATT-LARSSEN: And I'd add, particularly on the sub-state actor, al Qaeda for example. I think I could – if you could visualize it, this footprint of an al Qaeda nuclear plot from conception to realization would probably be something like a 9/11 type footprint, and so small, in fact, that it'd be analogous to trying to find Bin Laden and Zawahiri today, which of course we know we're still searching for. And the problem is very acute for intelligence for detection when the clandestine nuclear activity is not for a state program with all the things that go into a state program, but for a group that simply bent on producing one bomb and the intent we know – and I want to stress this – is a yield producing bomb. That is the intent. I'm not excluding, of course, a dirty bomb, or a radiological bomb. It'd be far easier. It presents other problems. It would even be smaller, but in fact we have very clear evidence that the intent, at least in al Qaeda's case, is nuclear.

WARRICK: Okay, there's our microphone. Let's come up here to the front.

Q: Hi, I'm Chris Kessler. I'm a retired State Department non-proliferation officer, and my question is, given, in particular, the comments just made about North Korea and Syria, but also the fact that we know that most of the Iranian procurement efforts were not through the Khan network, also they certainly made considerable use of it, do you think that a focus on Khan is really a focus on what may happen in the future, or is it sort of looking back at what was certainly a galvanizing event but is not in fact the principal area where we have a problem.

ALBRIGHT (?): I can speak on this a little easier because I'm outside of the government. We have to look at what we know. And so with the Khan network we know a lot, and so we can assess it and then look at the lessons. I think the lessons still apply because we still see similar activity. We see glimpses of it. But I also share your concern. We shouldn't be fighting the next war by looking at the last one. And so we have to keep in mind and be prepared for surprises. And that's why I think from my point of view why increasing our detection capabilities are so important, both through cooperative means like safeguards working with companies, but also through the intelligence community. And so that we can try to not be as surprised in the future.

Q: Thank you. Bill Potter. I want to thank all of the panelists for a fascinating set of presentations. I think arguably the two cases involving Georgia in 2003 and 2006 can be cited as, not the most certainly very important instances of proliferation significant illicit trafficking. My question to Mr. Mowatt-Larssen has to do with those two cases and the extent to which one can point to any kind of a dedicated supply network. I believe you've been quoted in the past suggesting that rather than being very despaired, kind of isolated cases that the supplier may have been the same and if there may have been dedicated distribution network, I wonder if you might comment on that possibility.

MOWATT-LARSSEN: Well, I think there's a lot we still don't know, and I think the fact that you had an incident in 2003 and then one again in 2006 involving reportedly material from the same sources means that – implies the problem's not resolved and that it's a very complicated problem. And I know that the Russian government, Russian officials are taking it very, very seriously as are we and that there's some cooperation in that regard that you'd expect in a case like this.

I would decline to characterize the degree of sophistication of the network. There're very different cases for the publicity that's out there. You know the 2006 case was a sting oriented operation, which I'm a little hesitant to characterize it as in the sense that if you have missing material from 2003 and you're not confident in 2006 that you've plugged the leak, I would hope you would go out looking for it if you can still acquire more material from that source.

And I would add as a comment, it's a problem that a lot of people are discussing today and I say this with the appreciation of complexities for the intelligence organizations, global intelligence organizations, how do you go about out there to resolve a situation like you have there in that case in a way where you don't stimulate the market or make the problem worse. The last thing you want to do is send people out and encourage sales of materials. But at the same time, you can argue that if you're not out there, then you're not in a position to see what might be available. So I think

there's a balance issue. I think we've got to be – the thing we certainly agree with all governments on is let's not use these issues to embarrass one another, but work it, and show our bona fides in terms of making sure that the problem is getting the materials off the market, not using it as against one another or for political purposes.

I just want to add one last comment that if you take the problem of nuclear materials and you apply it to the A.Q. Khan, in terms A.Q. Khan played in Libya, Iran, and North Korea, the problem really is what would happen if we were dealing with a sophisticated, dedicate black market network like a A.Q. Khan network. That's what I'm suggesting that is something we have to fear. I'm not saying it exists today. I'm saying that's something we have to assume and then go out and prove the negative.

WARRICK: Let's go here to the front.

Q: Hi, I'm Ed Lyman from the Union of Concerned Scientists, a question for Mr. Mowatt-Larssen. I appreciate the remarks you made about the problems associated with the increased production of weapons usable materials in the civil fuel cycle. Now, we work a lot in trying to keep our finger in the dyke and not increase what we think it's a problem that's already extensive. And so we were trying to oppose the growth of reprocessing in the world. But we run up against a very common view among policy-makers that the issue is really clandestine production, that diversion theft from the civil nuclear fuel cycle is not a significant threat. And that is fueling or justifying the expanded interest in reprocessing both in the U.S. and other countries.

So my question for you is our view that you need to model an adversary conservatively and assume that they will have the capabilities over a period of time in which an expanded fuel cycle will prevail, or are we being unrealistic? And I'll just give one example as I had an argument with NRC Commissioner Lyons over an exemption that they recently provided for U.S. reactors that want to use plutonium based fuel, where they, essentially, will exempt them from the physical protection requirements for category one materials based on the belief that it's not credible for terrorists to be able to steal mixed oxide fuel from a reactor. So that's my question.

MOWATT-LARSSEN: Well, I am certain from my experience in particularly the Department of Energy in the last three years that the last administration and I'm sure this administration is carefully weighing decisions made relative to reprocessing in nuclear energy and taking all this into account in a very serious way. I'm also sure that with lot more knowledge than I are taking into account ways of increasing our production of nuclear energy in ways that would be proliferation safe, and that's going to be very interesting I believe. I'm sure everyone here wants to hear more about how the Obama administration is going to balance this issue. But I saw no indication that the issue was treated lately or that wasn't being taken seriously with the best – informed by the best science of the threat.

One of the things that's hard to do in a public forum and I tried to always walk the line between hype and reality and particularly when you're in a situation you'd like to convey more information, for example on al Qaeda's threat, but you really can't, but to then relate what you do know in a convincing manner that you're not hyping a threat. The threat of reprocessing is real. It's

a question then how you balance that threat against the benefits of nuclear energy and whether it was in the last administration or this, I'm convinced all that's being looked at very seriously.

WARRICK: In the back behind you.

Q: I'm Stephanie Cooke of Uranium Intelligence Weekly and I'd like to ask a question about uranium, and, specifically, just mention briefly what David and I have talked about in the past, which is how Iran acquired the uranium it's using today, which was done back in the late '70s the deal was made. It was perfectly legitimate and it was done when the Shah was in power and then it was consummated after the Shah fell from power and it wasn't reported in the early '80s and it wasn't reported to the IAEA until 1991, I think. I think it's a lot harder for Iran to get uranium today because of the various sanctions that have been applied, but I wanted to ask if there's any consideration on what the panel views are of safeguards starting at the uranium mines. I'm thinking of particular places in Africa that are pretty wild right now and whether there's any thought being given to that. And the details, by the way, of the Iranian transaction are in our issue, which is downstairs if anyone's interested. But I did want to ask that because I think it's an important that Oppenheimer addressed and it's sort of just falling by the wayside over the years. So I look forward to your comments.

ALBRIGHT: No, I think it should start. That would – from my point of view, that would be one of the things to consider in revising safeguards. And the IAEA has experience in Africa looking at this kind of renegade minds. And so I think it's something to consider and to bring under at least the investigation of IAEA. I don't know if you want to start safeguards there, the actually material counting process, but certainly you want to bring in mines and much more. And I think one of lessons in Afghanistan and the Taliban is that horrible things can be happening in places where you traditionally would never even think to look. And so I think that what's happening in Africa is very concerning with uranium and should be looked at more carefully by the IAEA. But they need a mandate to do it. They can do certain levels of investigation. There're people in the room that can speak more knowledgeably to this than I. But they – ultimately they need mandates to do these things.

WARRICK: Let's come down here on the side. Yes, the gentleman with the red tie. I'm sorry.

Q: Jeff Abramson with the Arms Control Association. I'm intrigued by a couple of comments. I'd like you all if you would be willing to answer sort of political mechanistic question in terms of what you think are the two most valuable next steps and whether they are bolt on to existing institutions or something new that needs to be created. I'm particularly intrigued by the information sharing discussion, whether that is something – if that's a key next step—how would you institutionalize that? And your comment also about how the U.S. export control system may be squashing this. I have concerns about that comment, but the question around export control and information sharing, and is that a new system? Is that a new international system? So how would you sort of pick the next two steps moving forward from this conversation?

WIRTZ: The next step for me is clearly that there has to be a dialogue between U.S. authorities and industry, maybe in the form that trade associations first of all are sitting together with selected government officials to explore which next steps could be taken. The export control system that we have seen in the United States and we as a German company are also subject to U.S. export control regulations, we find the system much too complex, but to explain what in particular could be deleted from these complex regulations would lead a little bit too far.

I was criticizing export controls in a very general way, saying that catch-all controls cannot work in general because covert procurement attempts do not happen openly. So if the essence of such regulation is that a company has to have positive knowledge, then it would never occur. And so far we have to doubt about the value of such regulations. We cannot completely live without them, but they will not catch much – they maintain – they will catch everything, but, in fact, you don't catch anything because people in industrial companies will hardly ever know what the customer intends to do with their products.

Again, the next step that I would take is look at examples how industry-government cooperation is working in other countries. There are a few examples. The U.K. could be named as a leading example. We have good experience in Germany. We know that also Dutch companies work closely with their counter-proliferation authorities. So there are ample opportunities for exchange of information, hence to make very quick progress.

I think a good detail in my speech that the two main things that I see that are required are immediate steps to get access to this wealth of information that industry has to offer and to reduce the threat that industry is seeing of being investigated, prosecuted et cetera.

I hope that answers your question.

ALBRIGHT: Yes, I'm not sure I can do two, but let me do three. One is the universalized export controls and to make sure that countries have them. And then part of that is on a targeted basis to try to make them effective. And two places – or one place and a category that need a lot of work is China is a huge hole in this whole system, and there's need for a lot of work with China to improve their ability to basically implement their own export controls, and sanctions imposed by the U.N. Security Council on Iran. The second is countries of transit concern and essentially you want to have a strategy to force the sort of the networks back into their country of origin. You can never stop this, but it's better to have them operating from let's say Iran than from UAE or from Malaysia. So you want to push them back into their host countries.

A second one is that the additional protocol really does need to be a requirement. The NSG should make it a requirement for the supply of a reactor. U.S. law should mandate those kinds of actions by states. It should just become a norm.

And then let me just reinforce Ralf's statement. Information sharing here does not work well. Obviously the FBI, law enforcement authorities are going out and getting all kinds of tips from companies about other companies, but what Ralf is talking about is companies sharing their own information with the U.S. government without fear of being prosecuted for that information or

investigated. And that's a real problem here that does need to be addressed in the short term because what Ralf says, I believe, it's a huge amount of information. And I've seen it work in other countries where it provides just the kind of information you want to bust up these illicit trade operations. The names of the trading companies, the names of the people, their phone numbers, their addresses because this information is real time and it's very actionable and it just sits unused in this country, and yet we are one of the major targets of proliferants.

MOWATT-LARSSEN: Yes, I'd just add two very quick ones for that and of course coming from the intelligence side my first one would be that's got to succeed until a lot of these other things work and we just need a new approach. We need a new model. And the multilateral aspect, as much as I would hear groans from anybody in the intelligence world who tries to do multilateral intelligence and law enforcement, has to work. We have to find a way to make it work to share information more broadly, lower the level of the classification of the information so intelligence can be shared with police and vice versa. The second thing, which I think in the long term is the most important thing we can do, and Ralf hit very strong in his presentation, so I bleeped over it, is criminalization of – in fact, so did David – criminalization of this is a huge problem.

And I want to add my voice to theirs that there are requirements on the book for states in the U.N. or other organizations to do this, but states have to go take the next step and do it. And it's not just the A.Q. Khan network, it's the UTN network, it's Bashiruddin Mahmood and cohorts are free today. Yazid Sufaat and Rauf Ahmad two al Qaeda anthrax planners are free men today. There's actually a record of across the board of WMD, say, criminals who have not had done serious time for. And if you look at trafficking in black market materials, the only purpose of acquiring weapons usable material would be to put in a bomb. I think it should be obvious that the penalties should be much different than they are.

WARRICK: Okay, the gentleman we passed over in the back. Was that Matt Bunn back there? Matt?

Q: Two quick questions. One is what about people who are outside the established companies like Ralf's? We saw in the A.Q. Khan network case a guy like Gotthard Lerch, who left this company and established his own company in Switzerland and the South African similarly. They sort of had their own company. What can we do to convince states to sort of pay more attention to the people who have had access to this kind of technology who may have departed from the institute or the company that they were – where they originally had access to that technology.

Secondly, in a lot of these cases it involves basically corruption on the part of the supply networks providing a lot of money to people at a company who then end up falsifying end user documents or export control documentation or what have you. And I wonder if there's a need for targeted anticorruption programs in industries that handle this kind of sensitive technology.

WIRTZ: Yes, just one very quick point. I wished I could do much more against corruption and against criminal energy, but we have no silver bullet against this kind of procedure. We cannot protect or I cannot as a company official protect my company against criminal energy of individuals.

And as long as there's greed out there in the world and people want to make money, there will also always be criminal energy. That is an equation that has to go to government authorities who have the means to put fines and sanctions on people and to intelligence.

WARRICK: Let's take two questions back to back and we only have a couple minutes. Let's try to get a couple of questions at our panel, take the crack out of. Over here. With the red tie again.

(Laughter.)

Q: Yes, my name is Simon Henderson back in – 30 years ago, I interviewed and reported on Peter Griffin for the Financial Times at the time. And Peter Griffin was designated by the U.S. government in February of this year. So my question to Mr. Mowatt-Larssen is what took you so long? And my question to Mr. Wirtz is that for those of us back in the 1980s who were chasing A.Q. Khan and his procurement efforts – (inaudible) – was high on our list of baddies. Could you tell us something about the amount of equipment that you shipped to Pakistan and what it told you about the size of the centrifuge plants, or plant, that Pakistan was trying to make? Thank you.

MOWATT-LARSSEN: Yes, I'll just – (inaudible) – question, but what took us so long. I believe that the – and unfortunately can't get in a lot of the detail here – that the evolution of the intelligence effort against – (inaudible) – which you wouldn't have had in the Libya approach, those two things were inextricably tied. So the point at which you had what you needed to have to go to Kaddafi and convince Kaddafi to give up his nuclear weapons program is a very high bar, and secondly, to also be able to go after that to President Musharraf and deal with the A.Q. Khan aspect. And I don't think it could had been done earlier, particularly – and I have good intimate knowledge of how the evolution of this occurred and particularly with the added aspect of 9/11 and what it took to coordinate what we were doing in that with the approaches that then occurred at the political level and the negotiations that went into that. I think what the bottom line is we did in fact – it was a success. In fact that – there were some concerned we did wait too long. There were some concerned we should have done it earlier, even within the intelligence community, but I think the results, more or less speak for themselves with the caveat that there may be things, as it's been discussed here, that we still don't know and that may represent threats.

WIRTZ: Okay, maybe just a few facts that I remember. I joined the company in the early 1980s and I had a very limited insight at that time. But from what I remember, shipments from – we had two major facilities in Germany, one in Cologne and one in the Frankfurt area. I have some figures back to the times that we made shipments from Cologne. It was roughly a few millions in deutsche marks every year. So it was not really a very big amount, nothing that would have helped a company to survive, and, actually, also not a business that we badly needed to survive. It was simply at that time fairly legitimate business that was not put under any reserve by no government. The items themselves were not controlled. The end use was not controlled. There were no catch-all clauses over there.

From what I know today, I would say vacuum equipment that may have been shipped could be sufficient for less than 1,000 centrifuges.

WARRICK: Well, I hate this. We're totally out of time. Fortunately we do have a break now. So if you want to come up here and talk to some of our speakers, you're free to do so.

I'd like to please give a round of applause and thank you for your help.

(Applause.)

(END)