CENTER FOR
STRATEGIC AND INTERNATIONAL STUDIES
(CSIS)

"CYBERSPACE: A NEW SECURITY DIMENSION AT OUR FINGERTIPS"

WELCOME:
STEPHEN FLANAGAN, DIRECTOR,
CSIS INTERNATIONAL SECURITY PROGRAM

MODERATOR:
JAMES LEWIS, DIRECTOR,
CSIS TECHNOLOGY AND PUBLIC POLICY PROGRAM

SPEAKERS:
JAAK AAVIKSOO, REPUBLIC OF ESTONIA,
MINISTER OF DEFENSE

NOVEMBER 28, 2007

Transcript by
Federal News Service
Washington, D.C.

STEPHEN FLANAGAN: Well, good afternoon ladies and gentlemen, and welcome to today's Statesmen's Forum. We are delighted – first of all, I'm Stephen Flanagan, senior vice president here at the Center for Strategic and International Studies. On behalf of our president and CEO, Dr. John Hamre and all of our staff here, we're delighted to welcome the minister of defense of the Republic of Estonia, Mr. Jaak Aaviksoo, to address us on an important and critical issue confronting not only Western, but global security.

The minister, as you know, has served in this government in his current position, many of you may know, since early part of this year, having capped a long and distinguished career in the academic world as a theoretical physicist and as a leader in education at the university level. Prior to entering politics, he served as rector of the University of Tartu, 1998 to 2006, distinguished – and I had the pleasure of visiting that university and I should say not only a distinguished, but a really beautiful and quite diverse university that he was also the first pro-rector for after independence in '92 and '95.

Previously, he had served at that university as well as head of the Institute of Experimental and Theoretical Physics. And he was drawn into politics once before as minister of culture and education, first, and then minister of education in the period of 1995 to '96. He had had a long career, as I mentioned, as a researcher and scholar in theoretical physics, professor of optics and spectroscopy. I can't even pronounce it, as you can see. (Laughter.) Spectroscopy. He was a researcher at the Institute of Physics at the Academy of Sciences. He's widely published in a number of journals throughout – over 100 articles and journals on theoretical physics and other aspects of basic science.

He's been a visiting scholar at a number of institutes and universities in France, Japan, Germany, and also in Russia. And he mentioned he spent some interesting years in Siberia, I heard last night. His education is also from that was then Tartu State University in theoretical physics and also did work within the Academy of Sciences.

And he's received a number of awards from countries around the world for his work both in politics and in physics. So it's a pleasure to welcome Mr. Jaak Aaviksoo to the floor today. Minister, the floor is yours.

(Applause.)

JAAK AAVIKSOO: Mr. Chairman, the audience, ladies, and gentlemen, dear friends who you've gathered here to listen to what I think is important when we think about our common future.

I've titled my talk as "Real Threats of the Imaginary World." And it's really a pleasure to be here in Washington today. And even more so, I'm glad to be hosted by the Center of Strategic and International Studies and have the opportunity to present you the Estonian views on cyber security here at the Statesmen's Forum.

I'd like to start from a small trip back into the history. It's in here in the U.S. when the Wright brothers started to conquer the airspace. And we know what importance airspace now has for our national and global security. It's equally remarkable that the cyber space was born here a few decades ago when the first two computers were taught to talk to each other. The good news was that they were able to do that and to communicate the good news. The bad news is that now, they are able to communicate bad news to each other, not only between two or three computers, but hundreds and millions of computers worldwide.

So where we are today? We are in a world where, in addition to the classical dimensions of land, sea, and air, we have a virtual reality; we use the term cyberspace. There is similarly a manner as going out to the high seas created new global powers, as conquering the air space for defense, but also for global dominance, we entered airspace and further to the space. It is imminent I think that the future developments will see conflicts, attacks, if you like wars in this newly born cyberspace.

Differently from the three dimensions I have mentioned before – land, sea, and air – where we are more or less able to define natural borders, and to do understand what we mean by saying, we want to assure natural sovereignty of our national land, sea, and air space. The imaginary cyberspace has essentially no borders. As it was born, it was global. It was not only global in the sense of having no borders, but it introduced also unparalleled anonymity. As by now little legal – both national as well as international – legislation, and it's an essentially dimension which requires modest financial means to be visible and present in that space. That basically means that it's fundamentally asymmetric.

I think we are more or less have developed a joint understanding when we say what we mean by national defense in the classical sense. That is, to live in our secure borders within the national space and sovereignty imposed by our legislator and executive and judicial powers. Neither legislative nor executive nor judicial powers are as yet present in the cyber space. However, in the real world, we increasingly feel the impact of this imaginary cyber space on our every day life.

The synapses between the cyberspace and the real space increase in influence what happens in the real space, but increasingly more, also how we feel, what we think, how safe we are, and what possible and imaginary threats may threaten us. With this in mind, we can imagine that a simple or minute waves of electronic origin can cause as big a damage as a cruise missile or even a nuke. At least, it's possible and no one presently can exclude such things happening in the future.

We have entered a new era. And coming from Estonia, as you well know, it's not an imaginary, but a real threat that we experienced a few months ago.

The Estonian experience – of course, cyber attacks of different kinds, starting from classical hacking into databases and computer systems, spreading viruses, a new type of cyber attacks has emerged, attacking so far individual businesses, maybe also personal websites, sometimes more or less politically motivated, but never implemented on a national level. I think it's fair to say that the level of organization is political motivation as well as the level of coordination and the volume, which for a small country like Estonia, clearly reached national security levels, took place in the end of April and early May this year.

Most of you surely know that this was related to the political decision to move a Soviet-era monument or actually relocate it to a military cemetery because, over the last years, with raising and externally provocated conflicts between different interest groups in Estonia forced the government to relocate this symbolic place in the center of the Estonian capital. Most of the attacks were carried out against Estonian governmental websites and servers, but also against Estonian news portals, against two biggest banks in Estonia, and later all of the other commercial banks as well as several Internet service providers and telecoms.

Just for your imagination, at the highest moments of cyber attacks, the overall traffic from outside Estonia was more than 400 times higher than the normal rate. You may imagine what happens if you have 400 times more cars on the streets of Washington than usual. This was clearly felt on the national level. And taking into account the tensions around the relocation of the monument and the street riots that broke out afterwards, the people who were news-thirsty could not get access to online news. At the same time, the bank transactions that in Estonia to more than 90 percent are carried out via Internet were not possible.

We may ask what was the aim of those attacks? If they were aimed at making some real damage to our critical infrastructure, or even more specifically, attacking classified networks under the responsibility of the ministry of defense, then this was not the case. I think these attacks clearly showed that there is a huge potential to combine cyber attacks and the also recently emerged terroristic attacks. And I tend to term the events that took place in Estonia earlier this year as cyber-terrorism.

What made those attacks unusual was not their massive nature, but also the well-coordinated nature of those attacks. This was clearly not a spontaneous response accompanying political events. They had not included not only the events around the relocation of the Soviet-era monument in Tallinn, but also demonstrations and blockage of the Estonian embassy in Moscow.

These attacks were carried out in a very precise timeframe and, at large, were carried out by groups of organized computers, so-called bot nets or robotic networks, that were rented for that purpose and rented by clearly illegal groups that have hijacked a

number of computers worldwide, zombify them by malware that can be used attacking any target in the world, any time you wish, provided you have access to these networks and have the command of them.

So surely, behind those attacks were actors besides disgruntled or outraged civilians, also more organized structures. For the time being, there is no solid evidence whatsoever what we can use to putting the blame for organizing those events. Part of that fact is essential because it's related to the very character of the cyber space, its anonymity. Partly because this was clearly carried out in an undercover manner, all we can say is to see the correlation with other events that were at least partially coordinated and funded by the diplomat representation of our big neighbor.

Of course, here in the states, in some way or the other the biggest country in the world, whose defense budget as I recently learned is at least 1,000 times bigger; the same proportions apply to our national wealth. The extent of those attacks, however, posed a serious threat to Estonian sovereignty. These attacks didn't have the long-term consequences. Some of these attacks were efficiently neutralized and by large with the help of our friends both at home and abroad.

What were the objectives? As I said before, the impact of the attack was, first and foremost, of psychological nature and caused intimidation in the general populous. It created widespread confusion and miscommunication in the general public as well as making impossible online access to information use from Estonia in those turbulent times.

From that experience, I'd like to draw a few conclusions. Today, I think we can be fully confident that cyber attacks and maybe possibly cyber wars – although, I'm not willing to use this term since it has no real content for the time being – is not a possibility; it's not a theoretical concept, but may become and has, at least in one case, become a reality.

It, of course, makes especially the countries and systems the more vulnerable the more developed their electronic infrastructures are. But it's not never limited to those countries with developed infrastructures, at least any country who uses modern information technology is potentially under attack. We're used to those attacks at individual businesses, as said, sometimes political motivated if we think about the cartoon scandal of the Danish newspaper, for instance, but also in a number of other cases.

For us for the future, to handle those cyber attacks on the national level and linking the national security framework, it is very important to be able to define from what level these attacks can be handled as internal problems of individual businesses or individual organizations, maybe even individual national agencies, and from where on this has to be handled as a national security threat with corresponding responsibilities of respective authorities. One thing is clear; we have to tackle those problems in the nearest future. The threats, the probability of those threats, is rising in time.

Secondly, this threat is fundamentally global. Any country or any organization or part of it can be attacked at any time, at the same time. The attack itself is global. In the case of Estonia, we estimate that around one million computers were involved in those attacks at different times, being located in more than 50 countries worldwide. The biggest numbers come from the countries with biggest numbers of computers. This system is not selective and it's penetrating any national borders.

It is also – since the very nature of this global threat, it's impossible to try to fight it building imaginary marginal lines around our countries or agencies. This, in this cyber space, the location of the opponent is only rarely known. And its location is next to impossible to know beforehand. Even after a cyber attack, its specific origin is often very difficult to identify. Seeing as almost every computer in the world is connecting to Internet, perpetrators find it at times very easy to use malprotected personal computers to participate in attacks by controlling them remotely. By this way, a person from Austin, Texas, could be involved in an attack originating from an altogether different continent, even without knowing it.

Taking part in a recent security-related conference, together with Deputy Undersecretary Grimes, we asked the audience that according to statistics, there are at least two cyber terrorists in this audience because, most probably, their computers have been hijacked and can be used, attacking other computers wherever in the world. (Laughter.) The number in this room is somewhat smaller since the audience is less, but nevertheless, I think we have to think about to what extent we can be sure that our computers are not used for those purposes.

From here on, I'd like to continue with stating that there is a general lack of awareness and preparation against possible cyber attacks. Of course, in most ministries of defense and other critical infrastructure organizations, the people are ready and able to fight those threats from the cyber space. At the same time, the general audience, especially all of the computer owners are in most cases not reasonably well-prepared and aware of the possibility of those threats and to what extent they on one hand can be vulnerable, and on the other hand, willingly or unwillingly participate in those attacks.

It is a complicated question to what extent individual people or computer owners can be held responsible for those attacks. Will I just bring you a small mental exercise. In a war, in a regular war, guns are used as weapons to fight. In cyber attacks, computers are the weapons. We have made rules and regulations so anybody who owns a gun has to keep it from being used against third parties, either by leaving it at home on the table accessible to your children and them using it against their friends or classmates, then it's clear that we can be held responsible.

More or less, the same is true in the case of cars if we leave our cars' doors open and keys inside. If somebody takes the car and causes an accident or damage to third parties, we are held liable. What about computers? Are we authorized, in the future, to put the burden on individual computer owners to protect their computers from against

using them in cyber attacks or cyber wars? The question is so far unanswered. It clearly is an important question since it interferes with individual liberties to the extent that we have to be extremely cautious before legislating into that sensitive area.

Fourth, cooperation between public and private sector is vital. Our modern information systems and networks are fundamentally intertwined. In addition to defense-related classified networks, which in most cases are reasonably well protected, information systems of our critical infrastructure, which in very many cases are in private ownership, are not always subject to the same strict regulations. It's clear and most of the countries, to a different extent, are paying increasingly more attention to that.

On the other hand, it's clear that fighting those threats has to involve both governmental agencies and offices as well as the private sector in close cooperation. Even more so, we're taking into account the very nature of those attacks; they are speed; events happen in milliseconds or even in shorter time periods. They develop over minutes or hours. And so, fast reaction is essential. That basically means that the pre-prepared networks of a well-established command and control lines must be in place before things happen. We're only halfway, in most of the countries, to achieve that goal.

And last, but not least, the fifth conclusion – when handling the cyber attacks and possible cyber conflicts and cyber terrorism, the first obstacle we confront is the lack of conceptual space even in communicating what is going on. What was going on and what was happening? As I said before, a cyber attack is maybe the best-established term to denote attacks from an external force towards an concrete target. What about cyber terrorism, cyber wars, and other terminology? There is no agreement whatsoever on national and even more so on international level.

So the conceptual clarity is the first step on that way. The second is to try to agree on certain rules of how to handle and what can be considered a cyber crime. Again, this is a heavily under-regulated sector and it's very hard, even if we managed to establish the ones who can be held responsible, it is very hard to bring those people to justice and clearly more national as well as international efforts by our well-respected judicial authorities is necessary.

As I pointed out before, the problem itself reduces to a risk-management exercise. The possible events that may happen in cyberspace have to be handled and the risks minimized. Minimizing the risks is always brings with itself certain burdens, either by law or voluntarily taken upon different stakeholders. As I said before, these threats cannot alone be managed by governments; it has to involve both businesses, third-sector organizations as well as individuals. How to handle this burden sharing is a complicated issue that has to be addressed if we want to efficiently handle the possible extension of cyber conflicts in cyber space.

And from here on, there is a need to establish clear responsibilities between different stakeholders in that counter-cyber attack exercise. So, from these five major conclusions, I'd like to say a few words what we've done in Estonia on the national level.

First, we started and even speeded up the process of compiling national cyber security strategy. This document will be ready the end of this year, and I said before, this tries to conceptualize the phenomenon, define the critical infrastructure, put concrete responsibilities on developing necessary legislation, as well as asking from Internet service providers as well as telecoms and other extensive e-service providers to develop countermeasures to be able to confront any future attack.

As said before, it also includes certain guidelines for the private sector. In addition to that, in the June meeting in Brussels, the NATO defense ministers, partly on the proposal by Estonian governments, commonly agreed that urgent work was needed to enhance the ability to protect information systems of critical importance to the alliance. Estonia, on its behalf, has proposed more than a year ago, so long before the cyber attacks took place, to establish a NATO cooperative cyber defense center of excellence in Estonia. I'm glad that now, five countries have committed themselves to contribute and several others are in the process of negotiations to participate.

We are extremely thankful for the publicity we had due – or thanks to the cyber attacks early April this year. This is the positive side of the story – (laughter). We have modest resources; we could have never managed that publicity to our cyber activities in Estonia. Furthermore, we are – we are deeply convinced that increased international cooperation is needed to handle those new threats from cyberspace.

Interestingly enough, confronting the threats from the cyberspace, we have from the very beginning to adopt what we nowadays call a comprehensive approach. We see that the comprehensive approach is increasingly an issue in traditional conflicts, or at least semi-traditional conflicts, which NATO as an alliance and our coalition face in Iraq and Afghanistan. We see that boundaries become increasingly dissolved between the international and domestic affairs, between civil and military spheres, between the private and the public, between peace and conflict. This is essentially characteristic to every cyber conflict or cyber attack at the same time.

Who should raise those issues? Who should try to address those challenges? Since this issue has clearly become a problem of national security, at least those countries joining their hands in fighting traditional security threats should pay due attention to fighting cyber attacks in today, and increasingly so, tomorrow. NATO has played, for over 60 years, a leading role in guaranteeing security, in Euro-Atlantic space and, increasingly more so in modern days, worldwide. It has, I hope, both the willingness and the potential to address those issues. A number of countries have embarked on that process already, as I said before, the willingness to address those issues was underlined during the recent meeting of defense ministers in Noordwijk, and most potently, the most corresponding policy of cyber defense will be tabled to – on the summit meeting in Bucharest next spring.

Beyond the activities in the framework of NATO, I think also other organization, first and foremost at least from the Estonian point of view, the European Union as well as

the Council of Europe, should undertake steps in that direction. It's worthwhile to mention that there already exists an international convention on cyber crime that was approved by the council of Europe and that came in to force back in 2004. Unfortunately, very few countries have decided to join this convention; however, what we observe – the interest to work more closely, both in ratifying that convention as well as extending it to the new spheres of cyber crime and cyber attacks is underway.

However, it is also important to note that as it stands now, this convention on cyber crime of the Council of Europe is the only international agreement that concerns cyber crime. Taking into account the threats related to that, that's clearly on the critical. I think that having more signatories would be beneficial to every country that faces the emerging cyber security environment, and in addition to that it could act as a basis for any further legislation, as such arises in member states or further away.

As an organization of like-minded countries, the European Union is another actor that could do much in the effort of improving cyber security. Seeing as many NATO countries are also member of the EU, it would present a good opportunity to deal with the issues considered in NATO, also in the EU. And I am glad to say that the ministers of Justice of the European Union are increasingly paying attention to that sector and trying to legislate both at the European as well as national levels. Of course, it will be redundant for the European Union to replicate the work that NATO is already doing. For example, the EU could deal with cyber crime of commercial nature and as a part of that, implement legislation aimed at a wider range of issues that cyber security presents.

Furthermore, in addition to these international organizations, I am sure that cooperation between individual states, also bilateral relations can essentially contribute to facing that threat. However, we think that we have to find also new frameworks to work with these challenges. The approach to cyber security, I think, should be proactive, all-encompassing, and most of all, multilateral, a cooperative effort between governments, the private sector, and international organizations.

Now, I am getting a little bit more philosophical. When I was trying to draw a picture to resolve the threats and how to fight them, we have to be realistic in what we can achieve and what is proportional reaction to the possible threats. It is clear that as in handling crime, we can never achieve or legislate means and measures so that crime will disappear completely. There is always a tolerable level of regular crime as well as cyber crime and cyber attacks, beyond which the measures undertaken are too big a burden for the participating partners, as well as ineffective from the point of view of resources spent. However, whatever we undertake, a critical part of that, while we've failed at most, I think, even if we are able to identify the evil, is to bring the evil to justice. Bringing the evil to justice today is extremely hard, not only within national borders, however here certain success is possible and this country is a good example of being able to implement certain rules, but it's even more so on the international level.

Just one example – I don't know to what extent of confidence – we have identified as one of the attackers during the cyber attacks in Estonia as originating as

originating and working from the conflict zone of Transnistria, he openly declared that according to the laws of that disputable part of Moldavia, his actions and attacks were fully legal. This has been also officially referred to by some of the authorities we addressed to expel the corresponding person to Estonian authorities.

Dear Sirs and Madams, I'm starting to conclude. Globalization has made the world smaller; we are increasingly interrelated in everything that we do. The threats that are born in one part of the world reach our doorsteps faster than we wish that happen. We've had to reconsider a number of concepts that were able to handle conventional threats and conflicts. And we, I think, are increasingly aware to what extent we are sitting in the same boat.

Even more so, we are increasingly aware to what extent the problems we face are intertwined; intertwined in the physical and the cyber space, the legal space, national and international security interests, and so on. The more we are interrelated and intertwined, dependent on each other, the more we have to share jointly the responsibility for global as well as national and personal security.

I'm extremely happy standing here today, that Estonia, together with a number of other countries have joined into the Euro-Atlantic organizations standing for common values. I'm also sure that the number of countries and people who share the same values is growing in the future. I see that – I saw that happening over the last years and Estonia was one of those countries who joined these organizations this millennium. I'm sure that some of our adversaries today will be part of that alliance in the coming decades, however complicated that journey might be.

This, I think, is our common responsibility to move ahead despite the problems, despite the fact that not everything is easy and all –we definitely cannot solve all the problems as soon as we may wish, be it then the conventional conflict somewhere far or near from our borders, as well as the new threats that challenge us in cyberspace. But let me express my deep conviction that if we join our hearts and minds and brains, we'll be able to solve them, so thank you for your attention.

(Applause.)

JAMES LEWIS: Thank you. That was a great presentation. The minister has agreed to take a few questions. If I could ask if you could identify yourself when you ask your questions; that would help us and put things in context. And I'll take the – my name's Jim Lewis and I'll take the moderator's prerogative and ask the first question.

The attacks were a surprise; how did you react? Who was the first person you called? What did you do when you learned of this?

MR. AAVIKSOO: Well, to put it very simply, the attacks, I think most of the people in Estonia were taken by surprise. We were engaged with the conflicts we've had around the war memorial. And I personally learned about the attacks but where was I

unable to look at the online news, and then I called, what's wrong? And then I heard what was going on. However, at that time already, the informal network of meet level, department-head level officials were – had been informally organized long before those attacks took place in order to compile the Estonian cyber defense strategy – were already working with the attacks. They called their colleagues and friends in Estonia as well as abroad.

So, in the first hours of those attacks, a network of people was already working. So no formal decisionmaking to fight or defend these attacks were taken on the government or even on the ministerial level. I, on one hand, there is a question mark – to what extent all that was backed by existing legislation because steps taken in this process were in some cases clearly inflicting third-party interests. However, I am convinced that only a fundamentally networked system of cyber defense is effective in those cases, also in the future. So I think from that lesson we have to learn that we have to be able to defend ourselves as fast as possible, meaning in minutes and hours.

MR. LEWIS: Great, we have Mike Nelson in the back there. I'll identify you for yourself.

Q: Mike Nelson with Georgetown University. As you said earlier, this was primarily a psychological attack. They weren't actually bringing down machines – or they weren't doing damage to infrastructure. Do you have any assessment of how much damage was done psychologically? Are there poll results – (chuckles)? Are there any indication about what the Estonian people think of the Estonian government's response and whether there's more or less favorable reaction to what the Russian government's doing?

MR. AAVIKSOO: Let me put it like that. We, as you know there were street riots and the damage during those street riots, which had an unprecedented scale for Estonia, but which I'd say are quite usual if we look – a failed football match in Paris – (laughter). But nevertheless, I mean the psychological damage through those street riots was estimated – is hard to estimate, but the material damage reached, well let's put it up to $10 million.

The psychological damage is, of course, hard to estimate. The damage to the businesses, including banks and so on, this is also an indirect estimate, but it's also in the range of maybe $1 million or 2 or $5 million dollars. Psychological damage was clearly much higher than that, but of course bringing it down to number is somewhat complicated.

MR. LEWIS: In the middle there.

Q: I'm Pam Hess with the Associated Press. Could you talk about the assistance you got from the United States government? Who you reached out to and when? What it is that they did for you and what is was able to accomplish? And on the other side, can

you talk about the number of computers that were hijacked in the United States to be used in the attack?

MR. AAVIKSOO: First, the – in the early hours of these attacks, of course specialist consultation was the biggest help. Our next stage is help by blocking some of the servers and limiting the flow of the requests to the attacks to computers was the next stage. The third stage was sending specialists to assist in fighting future attacks. As I said, or maybe forgot to say, the first attack took place on the 28th of April, the next one, the massive one, on the 4th of May, and then around 9th of May was a third wave.

I think that the measures taken during the more than 10 days reduced the peak height of the attack in May by 10 times at least, so that we were pretty efficiently fighting the flows. Now, I'm sorry I forgot the last –

Q: The number of American computers that were involved with the – (off mike).

MR. AAVIKSOO: I'm sorry I can't specify that number. I can say – I can give you an estimate, and it's my personal estimate from the numbers I've heard, is that maybe 10 percent of these computers used came from U.S. Maybe that was less, sorry, but this is roughly an estimate.

MR. LEWIS: Okay, we have a question in the back.

Q: Yes, I'm William Henley with the Office of Thrift Supervision and I've got a two-part question regarding the lessons learned following this attack. And the first part has to do with business continuity; in the face of the attack, you mentioned about 90 percent of the bank transactions were interrupted, so as far as in the commercial sector, what lessons did you learn as far as business continuity? And we look at this country with our increasing dependence on things like voice-over IP and other things, so lessons that we can take from that.

And then the other lesson as the minister of Defense, what lessons did you learn as far as the ability for this to be a case study that if this were to be repeated, like a state-sponsored attack to be a diversion leading up to a military attack?

MR. AAVIKSOO: Well, first, the attacks to the Estonian banks. We have two major Estonian banks who are responsible for roughly 90 percent of the market and then four smaller ones who take their 10 percent rest. They were – the attacks were targeting one bank at a time, so they were shifting their focus from one to the other over different banks and times. To what extent it interrupted the services is hard to estimate; we asked the banks to give numbers and they were not very willingly having an official response to that request, due to understandable reasons.

But – so basically, the estimates were – they say that it was not too bad. But the effect was clearly psychological and I lost a number of colleagues and also businesses,

how they felt that and so I would estimate every second or third person in Estonia who tried to use that service couldn't do that during these three days of attacks.

And now as a minister of Defense, formally the responsibility of the minister of Defense in Estonia – the area of my responsibility was not directly attacked. So, I can say I was not attacked at all. However, of course, as being responsible for some of the related happenings in Estonia, including the relocation of the war memorial, so I was engaged politically to a very large extent, so I was from those who challenged or questioned the decision to relocate the memorial, they put the blame on me for initiating those attacks or provoking those attacks, so that was a clear political responsibility.

But more importantly, I raised the question for myself and for the Estonian National Security Council that where our responsibilities stop as the ministry of Defense in the case of massive attacks that have some national level impact, and if I know where my area of responsibility stops, can I be sure who takes over beyond that barrier? I mean, is that minister of Interior, or minister of Economic Affairs and Communications; who's responsible for the computing measures and response team? So, there's a question of sharing of responsibilities and this of course is an issue we have to work upon. And we do that.

MR. LEWIS: If you figure that one out, please let us know – (laughter).

In the green vest, please?

Q: Hi, Herb Lynn, National Academy of Sciences, did I understand you correctly to say that the attacks were largely undertaken by rented botnets?

MR. AAVIKSOO: Yes, that is the position we have now.

Q: How do you know that?

MR. AAVIKSOO: Well, it's a good question. I'm a physicist, but I'm in the computer sciences even less so somebody who's been working on the actual material. But I have reasonable confidence to the reports I've got.

MR. LEWIS: We had one in the – is that Ted there?

Q: This is Ted Bridis with the Associated Press. That was my question as well; can I add to that? How much does it cost to rent a million computers today? How asymmetric is this?

MR. AAVIKSOO: We had that discussion earlier today and since it's an illegal business, the prices vary, like let's put it like that – (laughter) – the prices vary for – it depends on the purpose and if you get it from a friend or from somebody who's acting on a purely commercial basis, and the risks related. I think it's a complicated question. But the rough estimate was that it may cost say 10 to 50 cents a computer, so it's not a very

big number and of course, doesn't require that big resources, but again, it's a very, very rough estimate, maybe accuracy to an order of magnitude or so.

Q: At least for a while the price has been dropping, so if you're interested – (laughter).

Q: Well, I assume this is renting access to somebody else's computer, so it's not renting the computers themselves.

MR. AAVIKSOO: No, no, no, what a botnet is – and I'm, again, not a professional in the field, but if you plant a malicious piece of the program, in any of the computers, it – this computer may become what I call a zombified one, so at any moment in time, when the computer gets a signal from outside, it can be triggered to send queries to whatever target the master has chosen.

So you put these botnets together over extended periods of time. You are the master of those computers for certain purposes and then you can sell that online to anybody who wishes to buy that. And this is very hard to discover as well, whether a computer is zombified or not.

So it's a phenomenon we have to live with for at least the time being. And I've heard different estimates how many computers have been hijacked, so to say. And I said before, when estimating the number of potential cyber terrorists in any auditorium, you may take the one percent guess as a good estimate; so one out of one hundred computer owners is potentially a cyber terrorist.

MR. LEWIS: I actually think the number might be a bit higher. And one of the problems is it's difficult to discover when you've been hijacked. The Netherlands police recently arrested two people who were bot herders, people who ran one of these bot networks. The network was 1.1 million computers. That's quite large, but it's not unusual, so it's the trend of the year in cyber crime.

Q: My name is Malcolm Ewing from the Brookings Institution. Can you tell us a little bit more about what the NATO center in Estonia that you mentioned is intended to do and how satisfied Estonia is with the response by its native allies?

MR. AAVIKSOO: Well, first, we tried to first use the competence that we have in Estonia in cyber defense. We have some academic as well as practical experience in the field. We do, we have to offer some expertise in the legal sector; we've been working on legislation concerning cyber crimes extensively. And this is one of the competencies I think we have to offer.

The response from other NATO countries is, I think, reasonably good in the sense that there are four committee countries and then seven in the process of negotiations. The so-called member of understanding conference will be convened early next year. And I think we've so far drawn reasonable attention so that we are pretty confident if we ask for

accreditation by NATO authorities of the Center of the Excellence, to get a formal status will be successful.

MR. LEWIS: All right, we had one in the back I think.

Q: You mentioned also about a comparison between vulnerable computers and the product safety that we have like for cars and for guns. A lot of those solutions were brought about at the manufacturing level with the guns having safety locks, installed by the manufacturer, seatbelts by the manufacturer. Is Estonia or Europe, are they contemplating any proposals to require manufacturers to make perhaps like lifetime licenses for anti-virus protection or things like that, a requirement?

MR. AAVIKSO: As far as I know, it's all speculative so far. But I mean, the question is up in the air and there must be some responses in the future to come because it's clear that this is one, maybe not the best, but one potential option to fight that problem.

MR. LEWIS: And I'm right in saying that the Office of Thrift Supervision is one of our financial regulators. (Off mike.) So we have a Treasury department regulator asking that. I thought your remarks on liability were very interesting and usually when you say liability in America, people scream and run from the room, so it was encouraging. (Laughter.) But it's a novel concept of making the consumer liable for misuse of their computer. Did you want to add anything to that?

MR. AAVIKSOO: Well, the consumer – are we really consumers if we are active players in the cyber space? And again, it's a question, not an answer, but I think we may look at these things from that point of view. We are active players; we make things happen in cyber space, so I mean, making things happen is always I think related to the question of liability and what the consequences are.

Q: Well, you can always turn off your computer.

MR. AAVIKSOO: Well, nowadays, you can't be sure whether you switch it off it's still not online. I mean, these are very, very tricky devices so it's not that easy.

Q: Gail Maddox, from the Naval Academy.

Can I broaden it just a little bit and ask you about the – is there been an enhanced perception of the threat amongst the populace? How has this impacted relations with certain of your neighbors? Could you address some of those issues?

MR. AAVIKSOO: Well, the cyber-attacks is not the biggest problem we have with one of our neighbors. (Laughter.) It's unfortunate that over the last five, but especially two or three, years the rhetoric and actions on behalf of the Russian Federation are not very encouraging. And I think that's felt not only in Estonia but increasingly so among European friends as well as here in the States. And this has also a defense-related

dimension; we see the strategic bombers flying around again, and the rhetoric concerning the legitimate interests in the near abroad is something that we are not very happy with. So it's a complex phenomenon, although I don't think that we need to panic.

I do have, personally, a lot of sympathy to the people in the Russian Federation. I think that the status where this country was left after the Yeltsin democratization was a very controversial one. To keep that country together, to wipe the increasing polity in Russia was a big challenge, and unfortunately the solutions taken are not maybe the best ones. But I still think that we should try to be reasonably optimistic but not losing our – keep our eyes and ears open to what's actually going on. So it's controversial. A lot of that, I still believe, is meant for internal use but not all of that. To what's going to happen in three years' time, it's very hard to tell. But I think we shouldn't panic, neither here and also in Estonia, although our bitter experience over the last 50 years is not making it easy to keep quiet.

MR. : Jerry.

Q: Gerry Epstein, here at the Center for Strategic and International Studies.

You said the targets were – you were not directly a target of this. But have you made, or has the Estonian government made, changes in its own use of the telecommunications infrastructure as a result of this?

MR. AAVIKSOO: Yes, we have. We've clearly decided to increase the security of our governmental information systems; we are pretty far with our e-government project, and we clearly identified the weaknesses of that system. And also, we clearly paid attention to the need to have more international cooperation to increase the security as well because a lot of that cannot be handled on the national level alone.

MR. : Time, I think, for one more. So maybe you'll be the last. Go ahead.

Q: You mentioned the one perpetrator in Moldova. What happened with him? You said that – you indicated that the government wouldn't do anything –

MR AAVIKSOO.: This is Transnistria; it's the disputed area in the Republic of Moldova which is, by now, at least practically occupied by the Russian troops, and this is not under jurisdiction of the government of Moldova. That was a public statement from one individual from that region, that he was behind those attacks and he was publicly announcing what he did and why he thinks that that will fall illegal (?), and so on and so forth.

We have also had – we asked for legal help from Russian authorities in two more cases where we've more or less identified the potential attacker, but no results. But, well, there is the Latvian-Anka (ph) case, which is even more serious and we are not very optimistic.

MR. FLANAGAN: All right. Well, I think the minister's opening comparison with air power and strategic bombing was very apt. Strategic bombing really began in 1914, when a very large balloon appeared over a Belgian city. And at that time, people were terrified but there wasn't a lot of damage, and no one expected what would come. So it's a very apt comparison for what we're going to face in the future.

My own view, for what it's worth, is that actually Estonia did a pretty good job in responding to these things; I held it up as an example of a place we could learn from. I'm not always sure the U.S. would have done quite as well, but you never know with these things, but from the outside it appeared to be a very effective reaction and response.

I don't know if you have any final –

(END)