FSC-PC.DEL/18/08
3 June 2008

ENGLISH only

**Check against delivery**

# Address by the Minister of Defence of the Republic of Estonia

## H.E. Jaak Aaviksoo

## to the joint meeting of the OSCE Forum for Security Cooperation and Permanent Council

## Estonian approach to Cyber Security: Estonian National Strategy on Cyber Security and Cooperative Cyber Defence Centre of Excellence

Excellencies,
Ladies and gentlemen,

I am very glad to address today's joint meeting of the Forum for Security Cooperation and the Permanent Council. In April, the Permanent Undersecretary of the Estonian Ministry of Defence, Mr. Lauri Almann delivered an opening speech on the occasion of Estonia assuming the FSC Chairmanship. As he outlined in his address, cyber security has a prominent place in our Chairmanship programme. Therefore, I believe that the topic of my address, "Estonian approach to cyber security", is very fitting.

Compared to other subjects, cyber security is a comparatively new issue. Yet the challenges that arise from it can be related to other, much more traditional security issues.

The problem of borders, which is prevalent in cyberspace also troubled the international community in the past, in the cases of maritime- and airspace. International borders were hard to define for the sea and air. For cyberspace, defining borders is next to impossible.

Dependence on resources has also been a strong characteristic of the world throughout the times. We depend on oil, electricity, a steady supply of safe water and food and many other things. In our modern societies, we have also come to depend on computers and cyberspace, and we are going to do it more and more. In a sense, unobstructed access to cyberspace is an important resource of the 21st century.

In traditional warfare, the identity of the attacker is not always apparent. Many centuries ago, privateers operated in the name of governments, but did not always identify themselves as such.

In a similar manner, guerrilla fighters and terrorists often do not carry any clear identification. One problem that the international forces in Afghanistan or in Iraq are confronting is that we cannot be sure that the opponents are always Afghans or Iraqis. In cyberspace, an attacker can be situated in Asia, but route his attack through servers in Australia, America or Europe. Therefore, the identity of the attacker is most of the time not clear and very hard to find out.

These are just some of the issues that go hand in hand with cyber security. Nowhere were these problems more evident than in the cyber attacks, which targeted Estonia from the end of April until the first weeks of May 2007. Our society is dependent on many essential things, which nowadays are done with the help of computers and internet.

News and communications, banking and governmental information systems were amongst the targets strongly affected by the attacks. It was hard to know where the attacks are coming from – there were no electronic men marching over an electronic border. Instead, we faced attacks from servers in as many as 75 different countries, including the USA, France, UK, China, Russia. We can only assume who was behind the coordination of those attacks.

When I mentioned coordination, I did so deliberately. There is simply no other way to explain the timing of some of the attacks, as well as the choice of targets. Moreover, groups of computers called “botnets” that are controlled through malicious software participated in the attacks. The biggest botnets in the Estonian attacks were approximately 10 000 computers large. The biggest botnets that exist in the world are estimated to consist of up to one million computers. Some of these botnets are available for rent on the black cyberspace market, but only through in certain circles. I could compare this with the black arms market – people who buy in bulk know what they are doing, and they always have a definite plan in mind.

We have to realize that any new technology can be used as a weapon. When people invented ships, there soon were warships. With cars and planes came tanks and bombers, and with nuclear energy came atomic weapons. This is not any different for computers.

When we use a computer, we should be aware that it can be used as a tool to cause trouble. Unfortunately, this awareness is not yet as widespread as it could be. This is one of the areas where it is easy, yet complicated to make progress. It is easy to try to inform ourselves about the possible security issues of computers and cyberspace. But it is much harder for the information to sink in to every level of the society. There is an immense amount of work that has to be done, and the OSCE as a multinational organization is a very good place to do it.

As a result of the attacks, Estonia has realized that we have to be more prepared, should such attacks take place again. The first step in preparations should be a detailed and in-depth document, which can describe the dangers that cyber attacks pose and how to confront them. In Estonia, this document is the National Cyber Defence Strategy.

The strategy details aspects of cyber security, which should be paid the most attention nationally. The basic requirement for maintaining any kind of cyber security is the understanding that every owner of a computer, computer network or information system realizes their responsibility of

taking good and reasonable care of the systems in their possession. This simple realization creates the foundation for a more secure cyberspace.

Of course, there is also still a very long way to go from there until we can truly say that cyberspace has truly become a more secure and safe place. The Estonian strategy details five general areas for increasing cyber security on a national level.

First of all, a frame of mind should be encouraged that everyday functioning of the society is dependent on information systems. Furthermore, ownership of these systems should come with a realization of the dangers and consequences, which can arise from not being able to provide the services tied to these systems. This means that the information systems governing critical infrastructure should be as resilient and secure as possible. Seeing as a part of this infrastructure is in the hands of private enterprises, better cooperation between public and private, but also between public institutions is necessary.

Secondly, competence in cyber security should be improved on a national level. Education, research and development in cyber security related field should be improved and encouraged. International cooperation in these areas is also important in staying up-to-date in this regard.

Thirdly, legal environment regarding cyberspace must be envisioned and brought into reality, both on a national and international level. A legal system capable to respond to any events that may threaten national security in cyberspace is crucial to maintaining a secure environment. Naturally there are many illegal activities already categorized, but grey areas also exist.

For example, if someone would steal a sensitive document from a safe, legal action would ensue in any country. Now, if the document would instead be stolen digitally from a computer, then some countries in the world have no legal basis that would declare this action a crime. Such events have taken place around the world, and taking into account the worldwide nature of cyberspace, these cases can end up in a grey area where it would be impossible to take legal action against the perpetrator.

Thus, international cooperation must go hand in hand with all what I have mentioned. Recognition and understanding that illegal actions in cyberspace should be condemned internationally is the first step that can be made. Joining international treaties and conventions which concern this topic is also very important. I would urge all countries to join the European Council’s Convention on Cybercrime, which is one of the few international treaties that exist on this matter. Only through international cooperation will we be able to move towards a more secure cyberspace.

Finally, raising awareness for the challenges and issues present in cyberspace will be necessary to make all of these things happen. Cyberspace must be demystified for people in all walks of life, in governments, the private sector – each and every citizen. To put it simply, we have to introduce the concept of “cyber culture” where becoming a good “netizen” would be informally recognized as a civic duty. Cyber security is also an area where nations can learn from the private sector, where many companies have long-term experiences and specialized knowledge.

Ladies and gentlemen,

I am sure you have heard about the NATO Cooperative Cyber Defence Centre of Excellence that is created in Estonia. In many ways the Centre is an extension of the issues that are singled out in the Estonian national cyber defence strategy.

First and foremost, it should be underlined that the Centre is not an institution with military aims. Rather it is a centre for expertise, scientific research and development, where the nature and various means of cyberattacks that have been used can be studied, in order to be able to protect ourselves better.

A very important point to make about the Centre is that it is a cooperation effort between countries that have recognized the challenge of cyber security. The fact that the Centre is multinational is of especially great value, as its concept allows both NATO member and non-member countries to join.

Just a few weeks ago, a memorandum of understanding between participating countries was signed in Brussels. I would hereby urge all interested parties to participate in the Centre, as we can not allow ourselves to neglect this issue. Following the signing, the Centre will go through an accreditation procedure, and is set to achieve operational capability in January 2009.

Not least importantly, the creation of the Centre has also served the purpose of informing the public about the importance of cyber security. That an influential organization such as NATO has deemed it necessary to establish such an institution goes a long way to show both inside and outside the Alliance how significant this issue is. It also gives a clear signal to the public that cyber security is something that can not be ignored.

Dear audience,

Today I have outlined the challenge that is security in cyberspace. I deliberately did not mention the question of defining cyberspace, which is a completely different topic in itself. I suspect that if we would start on this issue, we would still be discussing it here in this room tomorrow.

If it had not been for the onslaught of cyber attacks that hit Estonia, I would probably not be addressing you on this topic today. It took a “wake-up call” for everyone to realize that the threat is very real. Now that the international community has indeed woken up, I am hopeful that the momentum will not be lost.

What is important is that we should step up to this challenge. The need for international cooperation should be stressed, and I believe that OSCE as a large and influential international organization can play a big part in addressing this issue.

Thank you