‘Defining cyber-security:
The role of NATO in ensuring common defense’

Ladies and Gentlemen,

Thank you for the opportunity to address this conference.

I will not bore you with the genesis of NATO’s role in cyber defence. Let’s just say: it has been a long and hard climb. Today, however, we are moving fast on the road to take cyber defence where we want it to be – and where it needs to be: in the centre of Allied and partner attention. Cyber defence is finally shedding its image as a playground for geeks, and taking its rightful place as a “must-have” core capability for the 21st century NATO.

In my remarks today, I want to focus on the future – a future that will feature strong public-private partnerships and closer cooperation with partner countries as well as academia.

We all know full well: cyber defence is a cooperative exercise. It requires the close interaction of all key stakeholders, public and private; civilian and military; state and non-state; defence and homeland security. NATO is certainly not a “silver bullet” in cyber defence – but it has unique capabilities to offer to Allies and help them achieve enhanced cyber security.

Let me very briefly – in a telegramme-style – offer you ten points that describe the role that NATO has in ensuring common defense and where I see NATO going in cyber defence.

First, cyber will get even more attention from our highest political levels. Since the Lisbon Summit, cyber has been given much visibility by our Heads of State and Government. The next Summit will be even stronger on cyber defence. This should help us move forward – but it will also increase the pressure on us to do it right.

And this brings me to my second point: we have a robust Cyber Defence

Action Plan from last year that we need to fully implement. Currently that is clearly the top priority. All NATO structures will be brought under centralised protection. Last February, a 58 million Euro contract was awarded to upgrade the NATO Computer Incident Response Capability. These efforts now underway will significantly enhance NATO's cyber capabilities over the coming months. And since technology is not standing still, we cannot lean back: a continuous attention will be required also in the future to keep this capability up-to-date.

Third, it is critically important to be aware of how the cyber threat landscape evolves and have indications and warning before cyber attacks targeting our digital networks occur. The recently established Cyber Defence Threat Assessment Cell (CTAC), which will become fully operational in a few months serves as a most useful interface between the tactical/operational level cyber awareness the NCIRC Technical Centre and the warnings and analyses by the intelligence community. Our situational awareness could be further enhanced by using NATO as a platform, a sort of "clearing house" where key stakeholders, Nations and industry exchange relevant information and intelligence to increase our chances of early detection.

Fourth, we will accelerate our efforts in training and education on cyber defence, through our schools and specifically through the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn. The Centre could very well serve as a broad platform for Nations and industry to share best practices and lessons learned and run joint exercises. Our goal is ensure that an ever greater number of officers and civilians understand the cyber challenge. NATO has a fine tradition of educational excellence. We will build on it.

Fifth, capabilities. NATO is about capabilities, and cyber is no exception. To quote the famous military strategist – Ronald Reagan: "I once played a Sheriff without a gun – I was dead 27 minutes into the show". You cannot put it any better. But what does this mean in cyber terms, and what does it mean in times of austerity? It means that Allies need to re-prioritise. That they spend more on cyber even if they are cutting elsewhere. Some are already doing this; other must do it, too. Enhancing cyber defence costs money, but it won't break the bank. Besides, we can save money through multilateral solutions. If we can do it in strategic airlift; we can

also do it in cyber. For me, this would really put the “smart” in “smart defence”.

Sixth, we will integrate cyber defence into the NATO Defence Planning Process. This process is one of NATO’s greatest assets. It makes Nations through the development of force targets concentrate their efforts and build capabilities that the Alliance needs. It gives NATO its unique punch.

Seven, we will work even more closely with partner countries. Cyber defence is a cooperative effort, where no one, however powerful, can go it alone. You cannot build fences that are high enough to keep cyber threats away. NATO can do a lot more if it works with others. And we have a strong and large partnership network , which now reaches from Europe all the way to the Asia-Pacific region. 69 countries are connected through it – that’s more than a third of the globe. By working with these partners on cyber defence, we can shape the strategic environment in unprecedented ways. And we are determined to use this opportunity. Similarly, we are establishing standards for future military operations, which will have an impact not only on the NATO Allies but also on the military of our traditional operational partners.

Eight, we want to work more closely with other international organisations, in particular with the European Union. We would defintely do a major disservice to our members states if these two organisations were to fail to get their act together. We need to develop standards together. NATO has already embarked on that road for national CIS that NATO depends on. We also need to harmonise our crisis response procedures. Not doing so is a recipe for failure – and an abdication of our common responsibility to protect our citizens. That’s why we will continue to push for a new level of NATO-EU cyber cooperation.

Nine, NATO should move beyond its traditional communities and tear down the old separation lines between the defence and the homeland security communities. Cyber defence cannot be effective if we do not link the two together.

My tenth and final point: we will need more public-private partnership. Let's face it: More than 85 % of our cyber infrastructure is owned by the private sector. It is the private sector that produces the technology solutions that we need. And they are the ones who represent the first line of defence. I am aware that this is not NATO's traditional terrain. But let me be very clear: without more private-public partnerships NATO would be left behind the curve. And we want NATO to be ahead of the curve.

Ladies and Gentlemen,

Threats arising from cyberspace are increasing both in frequency and sophistication. Protecting our 900 million citizens against such threats is an enormous challenge. It requires a new understanding of collective defence; a new definition of core, essential capabilities; and it requires new ways of doing business with partner countries, other organisations, and, above all, the private sector.

Some have said that this is too complex a challenge for NATO to handle. I disagree. Yes, cyber is a crucial test for our Alliance: NATO can either stand up and be counted, or lie down and be counted out. But I can confidently say to you: We have no intention of lying down.

Thank you.

Check against delivery!