Ladies and Gentlemen,

I would like to welcome you all to Tallinn, Estonia. As you have been able to observe, we are a rather small and unassuming country, fairly advanced when it comes to Internet applications but nothing really too outstanding. Yes, Skype was developed by four young Estonians, after they invented Kazaa, which got them in trouble. We offer quite an advanced array of public services on the web – more than most countries. Estonians have come to consider Internet access more or less a right, manifested in near universal public access, including at the airport, for me a welcome change from the 10 euros you have to pay at most European airports just to check your e-mail. As I said, we are a small and rather unassuming but technologically advanced country.

We never really thought we would become a byword in the field of cyber security: After all, what could a small nation of 1.3 million with a GDP less than a number of companies like Microsoft have to say on such matters?

As it turned out, a combination of two factors led to our becoming a byword in this field. One was the high level of Internet utilization in society and the other the fact that we became the first victims of co-ordinated attacks on our Internet sites and more importantly, I stress, our Internet-based infrastructure.

Computer attacks, hacking, malware; all of these were issues discussed in the literature long before April-May of 2007, when we were deluged at a nationwide level by DDoS attacks. We found ourselves on the cyber security map because we were the first country to come under attack. Moreover, since humans think like David Hume said we did, we assume that there was a political motive in the attacks. So we became the object of politics carried out by other means, which as we know, was von Clausewitz's definition of war. Banks, government services, even emergency response phone numbers analogous to 911 in the U.S. and 112 in the European Union -- all were hit. In other words, we were victims of the first clear-cut case of use of cyberspace for aggression. That to this day we cannot for certain apportion blame for this attack does not mean (as some sillier people tend to say) that it was not important. Lack of attributability is, I would suggest, one of the key issues, if not defining features of cyber warfare, something that sets cyber warfare apart from all previous forms.

I don't really plan to dwell much on those attacks. They were, after all, fairly primitive. Distributed Denial of Service or DDoS attacks are the IT equivalent of clubs and rocks from a Palaeolithic world that rarely affects us.

Yet, as we know, even clubs and rocks can cause damage. That's why we have police. Our task, however, is not how to deal with policing issues but rather with security in a deeper sense.

Cyber warfare also differs in other ways from previous forms of Clausewitzean continuation of politics by other means. For one, it is genuinely asymmetric. If we have been talking about asymmetric warfare up till now in terms of Al Qaeda and other terrorist organizations, then I would suggest that terrorist asymmetry is relatively easy to deal with compared to the cyber world, where a rogue state or a group of rogue hackers can do enormous damage, if they are clever enough.

Let me turn this idea of asymmetry around for a moment to discuss the positive side of technology-based asymmetry, which actually underlies Estonia's developmental success. It was technological asymmetry that led me some 16-17 years ago to propose that Estonia invest heavily in increasing its Internetization. I got the idea from a reverse reading of a somewhat Luddite book, The End of Work by Jeremy Rifkin which argued that computerization and automation would render redundant huge numbers of workers as their work could easily be done by machines. Since as you might imagine, a nation of 1.3 million has some pretty serious existential doubts regarding its size, Rifkind's argument in reverse struck me as a solution: we were small but through serious and widespread application of computer technology we could become functionally, that is economically as large as much larger countries not as sophisticated in IT.

Secondly, I believed that computerization of society on a massive scale would allow us to leap-frog the yawning gap in physical infrastructure, the result of 50 years of underdevelopment or even backward development during the Soviet occupation. It would take decades to make up lost time in building roads, bridges and housing. But starting on a level playing field in IT in the early nineties we could leap to the front of the pack if we tried hard enough.

Unfortunately what worked for us – leaping to the front of the pack and being functionally larger than we physically were – is also available to those with more sinister intent than a small country that just wants to do well.

IT is the great leveller or to use the term applied to the Colt 45 in the 19th Century, the equalizer. You can spend hundreds of billions of dollars on defence and military hardware but you can still be paralysed or worse by hostile computer attacks by a small and relatively poor adversary, one that you may not even be able to identify; and even if you could, what would be the response? What would be the appropriate and proportional response, to use NATO terminology, to an attack from a country that in fact has virtually no accessible IT infrastructure, such as North Korea, which is widely held responsible (but not beyond a shadow of a doubt) for attacks against the U.S. and South Korea two years ago?

Since the primitive DDoS attacks against Estonia three years ago, we have seen a rapid acceleration in hostile tactics. One, a very logical extension of the attacks on Estonia was a co-ordinated attack on Georgia in August of 2008 when military or more precisely kinetic warfare attacks against Georgian units were co-ordinated with DDoS attacks on vital information infrastructure. This, a year after the DDoS attacks here, represented a major upgrade in tactics, equivalent to the combined ground and air-attack strategy in conventional warfare pioneered by Colin Powell in the first Gulf War where land and air attacks were co-ordinated to a degree never seen before.

But even that was primitive. The real danger theorized by many but not found previously in practice to my knowledge was the discovery of a logic bomb in the U.S. electrical grid, which if activated, would have taken out one third of the U.S. electrical system, if I can believe the Wall Street Journal and I have been assured that I can.

I need not go into all the cases of attacks, hacking, phishing, stealing etc… conducted for years against the Defense Ministries of NATO and other countries. You, or at least some of you, I am sure, know far more about all these things than I, a non-specialist, could ever hope to know.

I do, however, mention the three incidents – Estonia, Georgia and the U.S. electrical grid logic bomb because it is time for governments to get their heads out of the sand. These are three cases of actual or prevented aggression against nation-states carried out in cyberspace. Were they to have been carried out with kinetic weapons, we in NATO would be faced minimally with an Article 4 and most likely with an Article 5 scenario.

But we

A. Have no conception of how to define aggression in cyberspace or redefine it for cyberspace
B. Lack clear attribution to any political entity
C. Lack a response doctrine to apply were we to know who committed the aggression
D. Have not dealt with the possibility of asymmetry, i.e., What if an effectively military action was perpetrated in its entirety by a small group of unknown hackers

Which means that even before we can talk about the hardware and software side of Cyber Defense and Cyber Warfare, we have not developed a conceptual consensus. Indeed we don't even have a consensus that it is a problem, as I have discovered speaking with colleagues whose countries have a far lower level of computerization, not to mention that most people in politics even at my middling age don't quite get what the fuss of computers is about.

While I won't be holding my breath for a conceptional consensus, especially since national security issues are precisely those where consensus is most difficult to achieve, I do believe we need to begin to look at defence more seriously. Not at military defence but the defence of our populations.

For all the benefits of computerization and Internetization, we have failed to realize how vulnerable we are. If we recall all the ballyhoo surrounding the Y2K issue a decade ago, when we thought everything would grind to a halt because of an oversight, then it is truly amazing that we see virtually no mobilization in response to a very clear, very present and in fact already realized danger. As I was Minister of Duty on 31 December 1999 I can say that Y2K fizzled, at least here in Estonia. The sole memorable event that evening was that without warning, Vladimir Putin suddenly was made President of Russia.

Far, far more than a decade ago, our critical infrastructure, our electricity grids, transportation and mobile phone networks etc… are today so enmeshed with the Internet that any open society is vulnerable to complete failure. Computers operate virtually all of our critical infrastructure using Supervisory Control and Data Acquisition or SCADA systems that we rely on for our civilized existence. Now if we were scared half to death because of the Y2K problem, we should be in permanent fear thinking of what could happen if someone, some group or person maliciously and purposively attacked these systems, either through an implanted Logic Bomb or through hacking into the system. As all these systems are Internet-based, it is all possible.

As much of our critical infrastructure is also transnational – here in Europe all electricity grids are to some degree connected as are transport and communication networks – we require a transnational approach to infrastructure defence. We need to make our transnational computer-dependent critical infrastructure resilient, that is to say, if not impervious then at least maximally shielded from the dangers of an attack.

I realise that for computer experts this is a problem left to those often computer illiterate people known as politicians, who as we know, have little knowledge about IT, are loath to work on such issues in a transnational capacity and in general are more concerned about getting re-elected. Yet unless you, the experts, make a stronger case for defence of our critical infrastructure including such unpleasant issues such as regulation and standards, we will have little progress until it is too late.

This is my non-specialist's plea to you, the experts: Please do everything possible to alert your policy-makers, your elected officials to realize what the threats are. In NATO we spend hundreds and hundreds of billions of dollars and euros on defence against kinetic war, but we spend precious little on cyber defence. We fail to realize that a potential aggressor no longer needs to attack us with an army. Today you don't need an army, all you need is a key-stroke.

Thank you.