Welcome to Tallinn, a small city that nonetheless occupies an interesting place in the history of warfare. Ladies and Gentlemen, Friends,

Welcome to Tallinn, a small city that nonetheless occupies an interesting place in the history of warfare. Back in June 1219, on the Dome hill in Tallinn, we Estonians were fighting the Danes, one of many peoples to invade us. The battle was going well for us and badly for the Danes, and victory seemed imminent. But then, right when the Danes were about to give up, a flag with a red field and white cross fell from heaven. Grasping the flag before it could ever touch the ground, the king took it in hand, and proudly waved it in front of his discouraged troops, giving them hope, and leading them to victory. The flag, known as the Dannebrog, is still the Danish flag today, the oldest flag in use in the world.

Technology, in that case divine, got the better of Estonia in 1219. Later, Tallinn, which means Danish city by the way, became a walled city with moats, towers, parapets and portcullised gates. Which was fine until gunpowder, rendering here as elsewhere in Europe, walled defences obsolete.

As first time visitors to Tallinn will certainly discover, this is the home of one of the largest medieval old towns in Europe. Not because Tallinn itself was so large, but because when the larger walled cities in Europe were destroyed by aerial bombardment in World War II, Tallinn was partially spared… because in the larger bombing of 1944, the bombers missed.

All of this, by way of introduction, is to say that when technology is unexpected or changes, old forms of defence become obsolete.

This conference takes place two and half years after the DDOS cyber-attacks against Estonia in May 2007. More importantly, since 2007 there have been attacks of similar nature against Lithuania, Georgia and Kazakhstan. Government ministries and agencies, often defence related, in the US, Germany, France, and South Korea have been attacked as well. This has helped put cyber attacks on the international agenda to a much greater extent than previously.

The DDOS attacks, although not technically very complex, were of great significance, for several of reasons:

1. They were intended to create social unrest in response to the domestic policies of a democratically elected government, and so represent an intervention against a democratic system, but using hitherto unused methods as a continuation of policy by other means.

2. They were clearly organized, despite a whole lot of nonsense one can read in the press. They were organized because their intensity was neither stochastically random nor even followed a Gaussian or normal distribution. As the Estonian CERT (Computer Emergency Response Team) graph of the DDOS attack showed, they stopped exactly at 2400 GMT at the end of 9 May, no doubt completely unrelated to the historical significance of that day in some other country. When I asked the head of the Estonian CERT how this was possible, he answered: I guess the money ran out.

3. Evidence exists to suggest that the attacks may have been partially state-sponsored. The recent US report of the Cyber Consequences Unit examining the cyber campaign against Georgia suggests that the organizers of DDOS attacks against web-sites in that country had advance notice of Russian military intentions. In a word they were apparently co-ordinated with a country's military and so constitute a possible infringement upon national sovereignty and, more alarmingly, may well illustrate an a new stage in the development of cyber warfare. A Public-Private Partnership, if you will.

What is perhaps most significant about the recent attacks are the issues they raise and the weaknesses they expose. These are no longer matters of theoretical abstractions, but real life issues that urgently require answers and action.

We have seen evidence that from a technical standpoint, cyber attacks are growing more complex, moving beyond the relatively unsophisticated DDOS type. There are worrying signs that their use by state and non-state actors is growing, not diminishing.

Modern societies rely on Internet solutions. They have become an essential component of everyday life—of how we do business, communicate, govern, and go about our daily affairs as citizens. For a country like mine, the internet has been a crucial motor of development and modernization that has allowed us to leap-frog from Soviet backwardness to cutting edge technology.

The development of an effective response capability against cyber disruptions—whether intentionally man-made or not— requires a major cooperative effort both within and across countries: it demands a broad participation of domestic actors, private and public, as well as concerted action by states, internationally and regionally.

I would first like to touch upon Domestic-Level Action.

There are three major issues here: raising public awareness of cyber security and threats; public-private cooperation; and public-administration consolidation.

First, the basis for effective decision-making in this field requires targeted efforts of raising public awareness. People need to be made aware of the risks of down-loading material from dubious sites.

We should not, however, limit our efforts merely to promoting safe use of Internet among private individuals. Our efforts must also embrace decision-makers and opinion leaders on such matters – politicians, business leaders and journalists. Politicians in many countries have little experience with current developments in computer technology. The business sector is not necessarily interested in IT developments outside their immediate application in ones own market niche.

In other words, the issue of cyber-security must be brought into the mainstream of the national-security discourse. Eventually it will be an issue in the mainstream in any case but it is clearly in our interests to have it led by us, not by events.

Second, at the national level we need far greater coordination between and among the various national authorities, including law enforcement bodies, regulators, emergency response authorities and military.

Here I would frankly state that I am worried: We seem incapable of adequately apportioning national responsibility and competence in this area. Some agencies do not wish to give up their turf, or don't want others to encroach on it; other agencies on the other hand lack the capabilities to deal with issues that thanks to modern technology now have fallen in their laps.

In other words, the division of responsibilities among government agencies that was appropriate with one set of technologies may no longer apply. Who should be responsible for moats, parapets or portcullises of a Medieval city is not an issue when you are being bombed by the Soviet Air Force, as we were in 1944.

Specifically, horizontal cooperation between economic and social institutions and law enforcement authorities is particularly crucial.

And finally, third, private-sector involvement is absolutely indispensable. No effective or workable solutions can be attained absent public-private partnerships.

The key to any adequate strategy, however, rests in actions at the International level. After all, cyber-attacks, cyber-crime, cyber-terrorism are almost a priori cross-border issues. Those responsible for malicious cyber-acts need jurisdictional lines to hide behind. Given domestic national capabilities, you would be a pretty stupid cyber-terrorist to attack institutions in the country you live in.

The substantive issue we need to address is international cooperation in the field of Critical Information Infrastructure Protection.

We have witnessed a number of successful initiatives: The European Convention on Cyber-crime and the European Convention for the Prevention of Terrorism, adopted under the auspices of the Council of Europe are excellent examples of success. The European Union has passed some important regulations as well.

These treaties are not only pan-European but also open to non-European countries. The convention has been ratified by USA; Canada, Japan and South Africa have signed the Convention on Cybercrime, more than 100 countries worldwide use it as a guideline for developing legislation.

The willingness of a country to be bound by the European Convention on Cybercrime almost serves as a litmus test for a country's preparedness to cooperate in this field. In this light, it is extremely regrettable that Russia has chosen not to be a party to the convention.

There are those who claim that, as it stands, the regulatory framework is underdeveloped, that adequate protection is not attainable without additional restrictions.

On the other hand, there are those who maintain that no additional regulations are required, advancing the notion of an informal or self-regulating framework—after all, the very purpose of the Internet is to dismantle obstacles to free exchange, not encumber it. There is perhaps a partial truth to be found on both sides.

In enhancing the international regulatory framework, we must exercise care and avoid rushing into solutions that will prove to be unworkable or ignore the complexity of the network they purport to regulate. While suggesting new forms of legal regulation we must also be mindful not destroy the free exchange of ideas and freedom of the speech on the Internet.

And now, Ladies and Gentlemen, the question is: where does all this leave NATO?

We all know from recent history that politically motivated cyber assaults can take a variety of forms and range in their sophistication and targets. Since those attacks a number of countries have revised their cyber strategies and begun to emphasize the need for cooperation as part of an effective cyber defence.

Article 5 provides the ultimate mechanism of international protection in case of an armed attack against NATO nations. Recent cyber incidents have, at least in the opinion of decision-makers, not (yet) reached the threshold of an armed attack, but are still a great concern to the international community. In other words, they have been a serious problem but in terms of damage done, not yet equivalent to a more conventional attack. But we need to think about these issues, for an electrical grid taken out by a missile or a virus remains an electrical grid taken out. The first is clearly an Article 5 event, the second probably not. To make things even more ambiguous, think of an EMP pulse delivered by a tactical nuclear weapon solely for the purpose of knocking out part of a country's communications and electrical grid. The delivery is article 5, the effect equivalent to that of malware.

While creating "cyber Article 5" preparedness (which is becoming NATO's "niche" in the global cyber security agenda as opposed to the EU or COE), it is important to see collective defence as part of cyber deterrence in a wider sense (involving law enforcement, information infrastructure providers and information society stakeholders).

Thus, in questions related to international peace and friendly relations in cyber domain, the implementation of Article 5 is tightly related to how nations will perform on "Article 4 preparedness" – i.e. general cooperation on combating cyber crime, exchanging information about threats and defences etc. Collective defence will reside in individual defence. Individual defences (by country, organizations, entities) need to be coordinated and concerted to avoid legal gray areas that allow "evil-doers" (as in the case of so-called "patriotic hackers" or outright espionage) to escape legal accountability.

Collective defence mechanisms cannot be called in as "correction of mistakes" or lack of preparation on a national level. Thus, every nation needs to consider their part in cyber security law and policy potentially leading to international developments in the field.

In this context, implementation of Article 5 will be closely related to implementation of Article 4. Once a cyber conflict actually crosses the Article 5 threshold (and I should point out there is no need for sophisticated predictions – if it happens, we will know it), the legal and policy mechanisms created in peacetime and used to foster Article 4 cooperation will be the key basis for coordinated response.

This is not to say that NATO and ally nations need not think about how to implement Article 5. That is to say, think through what the threshold of involving NATO is, what “homework” needs to be done first by the country under attack and so forth. But because of the nature of information architecture, militaries will have limited capabilities in providing effective measures – especially where the targets include private and critical infrastructure or potential dual use objects.

Therefore, Article 5 preparedness starts with Article 4 preparedness – determining what potential responses can be taken within a country and between the countries, what is the balance between military and other types of involvement in conflict resolution. Furthermore, issues such as proportionality of response, consensus of the Allies as regards what consists the appropriate severity for NATO to take any action, and what type of force and action will be engaged, need to be considered. Not to mention the issue NATO has already had to grapple with in the post 9/11 world: who is responsible? How do we determine who is responsible? And what do we do when there is a disagreement within NATO about responsibility, as imagine there might well be.

In closing, I would like to thank the Cooperative Cyber Defence Centre of Excellence for organizing this event and to warmly welcome you in Tallinn and Estonia the home, not only of the god-given Danish flag, but also, and not incidentally, of Skype, but also the first on-line or e-elections and equally unincidentally, the first documented cyber attacks against a sovereign nation.

Thank you for your attention.