Keynote, Jarno Limnéll, 29.9.2017
Tallinn Digital Summit

Ladies and Gentlemen,

All across Europe there is much talk about cybersecurity. But precisely how much talk? I did a little research of my own. The word “cybersecurity” is mentioned in news and articles, in all languages of EU Member States, across the whole EU area. There has been a significant increase in the number of articles written in recent years. For instance, in 2014 there were approximately 41,000 articles related to cybersecurity. So far this year, up to the end of August, the number has already passed 114,000. It is worthy of note that this year’s cyber news has potentially reached over 105 billion people. As has been made clear in the EU’s reviewed Cybersecurity Strategy, cybersecurity today covers a very wide area indeed. I refer to you this word cloud which reflects the themes discussed in the media about cybersecurity.

The European Union now seeks a new direction and content. And rightly so. Towards this goal, which is closely linked with digitalization and security, Tallinn offers us an excellent framework to take things forward. Our actions, however, will only be decisive when we create a competitive, prosperous, coherent and secure Europe – for every European citizen. I believe that Europe has much common ground to come together, to successfully tackle all the challenges that we face, and to make the most of all opportunities.

There is one thing I wish to particularly emphasize: European citizens expect to receive protection from the EU and want to feel secure in Europe. They also deserve it, because every European has the right to security. Our shared values must be defended in both the physical and digital worlds.

We, the people, are now developing technology more quickly and radically than ever previously in human history. The development we see in different disciplines is gigantic and the effects of technological development on our lives will be very significant. To sum up, one could say that technology changes almost everything, and everything that can be digitized will be digitized. Changes are already to be seen in social structures, in business life and in the lives of everyday European citizens.

This digital century is a time of remarkable opportunity. We are taking giant steps forward like walking on the moon.

I don't believe that security should be understood only in terms of risks and threats. Rather, security is an enabler for innovation, growth and prosperity. Security – cybersecurity – is something positive when properly taken care of. We should therefore view the cyber matter as a digital and technological enabler. Cybersecurity is a precondition for the whole digital economy and a unique selling point for Europe which we need to capitalise on. You cannot have a Digital Single Market without ensuring its security. Therefore, we should consider cybersecurity as a core element of Europe’s whole digital infrastructure. With this mindset, Europe will become a global leader in digital technologies by 2025.

It´s good that the EU's new cybersecurity strategy emphasizes - quite rightly - the “Security by Design” principle. Smart devices are not that smart if they are not secured. The positive promotion of the benefits of digitalization requires built-in security for devices, systems, architectures and services.

In addition to the "Security by Design" principle, the "Ethics by design" principle needs to be highlighted. This is essential since, with the rapid development speed of artificial intelligence and robotization, it is no longer a question of what machines can and cannot do. It is rather a question of what they should and should not do. Ethical issues related to the development of technology are clearly becoming of greater relevance. It is, for instance, a question of how to bring greater transparency to the ever increasing number of algorithms that affect our thinking. Or, to take another example, what kind of ethical rules should govern the way that self-controlled cars are programmed?

It is also important to identify the cyber risks and threats. Large-scale manipulations of big data, the innovative practices of cyber criminals, cyber attacks targetted at critical infrastructure, and massive data leaks are all potential threats inherent to any digital society. Cyber tools offer an attractive weapon to those with malicious intentions – they are relatively inexpensive, effective, high-impact, difficult to predict, and hard to trace. If technology-based threats and attackers are agile and highly innovative, so must be those who defend against them.

Personally speaking, I am particularly concerned about deliberate cyber assaults at the very heart of western democracies: cyber-enabled influence on elections. The risk to our democratic processes is real, and, when assessing the hybrid threat, elections have become key targets. We are, however, already a step behind both malicious cyber-technical and cyber-psychological intentions if we prepare ourselves only for the forms of interference that we have witnessed thus far and felt in elections. I believe that the new European Centre of Excellence for Countering Hybrid Threats, which was recently founded in Helsinki, will provide the additional information necessary for making these estimates and preparations.

In recent years, issues relating to cyberspace and its uses have risen to the highest levels of international politics: cyberpolitics. It is becoming increasingly important to view cyberspace as a political domain. This is something that is often neglected or forgotten. I attach great importance to the creation of a powerful political deterrent to cyber hostilities against EU member states. Any would-be attacker must know beforehand that the political will of the EU, with various options for counter-action, can be found in our response to all such attacks and hostilities. The EU has pledged to begin development of what is called a 'Cyber Diplomatic Toolbox': a framework for joint EU diplomatic responses to malicious cyber activities. The initiative is welcome, however it falls far short of what is required. First, there are usually no “cyber-only” operations. In most cases it is likely that other influencing instruments will be deployed simultaneously; this must also be kept in mind when considering our responses. Second, Diplomatic ways of responding are important, but there are many other ways too. A comprehensive EU framework with different response options, more than just diplomatic tools, is what we need. It is also important to consider what precisely constitutes an act of war in the Digital Age.

The human being is the most valuable resource in cybersecurity and the value of talented individuals is increasing. It has been estimated that Europe will face a shortage of 350,000 cybersecurity professionals

by 2022. We will need to recruit the best experts available, and be able to train them far more comprehensibly than we do today in the different areas of cybersecurity expertise. This is a vital issue for European cybersecurity, and for its future. The global Arms Race for talented cybersecurity experts is already well under way.

Let me please emphasize one final important issue. Without a robust and secure cyber marketplace where European businesses can trade in confidence, there will be no adequate level of European cybersecurity for anyone. There is a great need for self-sufficiency in European cybersecurity - different products, solutions and services. If we fail to do this, it is difficult for me to foresee in Europe the level of trust needed to ensure our success in the digital world.

Fellow Europeans,

I wish to thank Estonia for leading the way in harnessing the potential that digitalization offers as well as for your advancements in developing robust cybersecurity systems. You have a model that it would be wise to follow. I believe, for instance, that many nations are now following closely your pioneering steps, after you launched the World's first data embassy.

In closing, let me emphasize three key words that are essential to ensure a safe and secure digital Europe.

Firstly, *trust*. Security, in any domain, is closely linked to trust. They go hand in hand – you cannot have one without the other. Without adequate trust, people will lose confidence in the digital marketplace and economic growth will be affected. Smart European citizens will not embrace technology they do not trust. Instead of asking how we can strengthen cybersecurity within our digital Europe, perhaps we should be asking the question how we can strengthen trust.

Secondly, *cooperation*. Cybersecurity requires team effort. For example, for us to effectively tackle cybercrime requires more active cooperation across country boundaries and within communities. Everywhere from our national and international law enforcement agencies, to cybersecurity authorities, to those operating in the private sector. Cybersecurity calls for greater human, technical, legal and institutional cooperation. This collaboration also needs to be reflected in a stronger sense of European solidarity.

And thirdly, *responsibility*. Cybersecurity is everybody's business. Every EU Member State, European business and European citizen must know their responsibilities in this matter. A big problem is that EU countries differ in their level of cyber-readiness, but we can resolve this situation together. Cybersecurity is, in principle, a matter of attitude, and our attitude must be right when we create a responsible European cybersecurity culture. Europe should function as a single European cyberspace.

I believe that trust, cooperation and responsibility are inseparable from our shared European identity and our European cybersecurity. Now and especially in the future.

Thank you for your attention.