Toomas Hendrik Ilves
Opening address at Munich Security Conference Cyber 31 January 2014

When the MSC for the first time discussed cyber security in 2011 the President of a small European country stood up and said: "this is the first time, but I assure you, it won't be the last". That was a mere three years ago. Two weeks ago, in a poll of senior employees within the White House, Pentagon, Congress and the defense industry, forty-five percent of respondents named a cyber attack as the single greatest threat to the US. This was nearly 20 percentage points above terrorism, which ranked second at 26%. No doubt a poll of senior officials in the Alliance or in the EU today would yield similar results.

This represents a sea-change. To understand why, we must re-examine the nature of security in an age of "cyber", for want of a better word. For cyber is a domain that extends far beyond the traditionally military-based considerations of security. Indeed so far, that its use and abuse impinges on the very core democratic values of the Alliance and the Union.

The more Information and Communication Technologies, or ICT for short, penetrate our ways of life, from the financial sector to our daily use of smart phones; the more we rely on SCADA or Supervisory Control and Data Acquisition systems to run our power plants, traffic lights and supermarket milk supplies, the more vulnerable these become to malicious digital attacks. To immobilize a nation, to render it incapable of defending itself, attackers no longer need military, kinetic weapons. Nor do these same weapons offer us defence. Today this holds true theoretically. Nations continue to buy tanks and rockets, but there have been enough tabletop cyber conflict exercises as well as real incidents to know what is possible already now.

*

I keep no tally of cyber attacks, hacks and espionage, but it is quite clear the issue, as I mentioned, has come to concern the highest levels of political leadership in the West to a degree we have never seen. We have witnessed a 17-fold increase in cyber attacks on American infrastructure from 2009 to 2011, initiated by criminal gangs, hackers and nations. In 2012, the US Department of Homeland Security announced an "alarming rate" of increase in attacks against power, water, and nuclear systems. On this side of the Atlantic we are less

forthcoming about numbers but we know for example the destruction of files in some 20,000 Aramco computers, imputed to Iran; there have been "distributed denial of service" (DDoS) attacks on the New York Stock Exchange, hacking during the missile attacks against Israel.

Estonia has faced these issues for what is a long time in cyber history. We were the first known target of politically motivated cyber attacks, in April 2007, when the websites of the government, Parliament, banks, newspapers, TV stations and other organizations were inundated with DDOS attacks that rendered them unusable. By today's standards they were quite primitive. Seven years later, as computing capabilities and IT dependency has mushroomed, so have our vulnerabilities.

In Estonia we can see a version of the interconnected and computerized future that is inextricably a part of the fundamental operations of society: 25% of the electorate votes online, nearly 100% of prescriptions and tax returns are done online, as is almost all banking. Estonians have given 140 million digital signatures, and last December, Estonian and Finnish PMs signed the first international treaty to be signed digitally. Adding to this near 100% broadband coverage and countrywide Wi-Fi, Estonia is one of the most wired countries in the world. What allows us to do this is a a secure identity based on a universal, secure Public Key Infrastructure with two-factor authentication with RSA 2048 encription. Our secure identity is a topic I alas have too little time for here, but it works and I believe to be the basis of any secure system.

As a country so dependent on digital solutions, we cannot help but be a proverbial canary in the coalmine. Today, almost everything we do depends on some kind of a digitized system. Our critical infrastructure — our electrical, water or energy production systems and traffic management — essentially interacts with, and cannot be separated from, our critical information infrastructure. As systems become more complex, threats become more sophisticated.

With cyber attacks, unlike in conventional warfare, it is often impossible to identify the attacker, and thus to know how to retaliate. Or against whom. In the modern digitalized world it is possible to paralyze a country without attacking its defense forces – the opponent could be ruined by simply bringing its SCADA systems to a halt. To impoverish a country you can simply erase their banking records.

Thus cyber security means we must defend the entirety of our societies, we need to reconsider much of pre-millenial thinking on defense and security. Non-military cyber threats can no longer

be conceived in terms of classical warfare – the traditional military paradigm remains necessary but is no longer sufficient. The whole of ICT infrastructure must be regarded as an "ecosystem" in which everything is interconnected. It functions as a whole, thus it needs to be defended as a whole. In Estonia we have been compelled to include in our security thinking domains never previously thought to be.

*

There are other pressing issues as well. In the past half year we have seen how different the digitized world can be when it comes to our most fundamental tenets about the role of the state and it relationship with its citizens.

In the 1960s Marshall McLuhan said we live in the Global Village. In the Television Age, this meant events around the world such as the Vietnam War could be seen by all in our living rooms. But the metaphor was incomplete. In our living rooms one could follow what was happening elsewhere, but you yourself remained anonymous. It was not yet a village.

Internet technologies have changed this. Today we do live in a Global Village. Governments, Google, the apps on your smartphone, your creditcard swipes make you an open book, just as in a small 19th Century village. Constant and intimate surveillance, the 1948 vintage fictional dystopia of two way television in Orwell's
1984
, today is enabled in every computer or iPad, unless you tape over its camera. Mobile phones are microphones that also can pinpoint your location. Big Data knows and can deduce more about you than Big Brother ever could – even if you are pregnant, based on your credit card swipes.

Yet there is another side to this. When internet thinker and Grateful Dead lyricist John Perry Barlow addressed governments in 1996 in his Declaration of the Independence of the Internet, announcing "Your legal concepts of property, expression, identity, movement, and context do not apply to us", he was right. They do not apply and we see the result (He left out privacy, I might add).

We could describe this state of affairs using Thomas Hobbes' characterization of the anarchy of

life in the state of nature as a war of all against all. Hobbes wanted a ruling sovereign to resolve this but in democracies we rely on John Locke's solution positing a contract between government and the citizenry, which underpins all modern democracies. The problem is we have no Lockean contract between the government and the citizenry in the cyber realm. Thus today, again, we are in the midst of a massive debate on what liberal democracies can, should and should not do with the extremely powerful technologies they possess. We are again living in a State of Nature. Our world is Hobbesian. We need our Locke, Jefferson and Voltaire for the digital age.

Personally, I think much of the problem we face today represents the culmination of a problem diagnosed 55 years ago by C.P. Snow in his essay "The Two Cultures": the absence of dialogue between the scientific-technological and the humanist traditions. When Snow wrote his classic essay, he bemoaned that neither culture understood or impinged up the other. Today, bereft of understanding of fundamental issues and writings in the development of liberal democracy, computer geeks devise ever better ways to track people... simply because they can and it's cool. Humanists on the other hand do not understand the underlying technology and are convinced, for example, that tracking meta-data means the government reads their emails.

C.P. Snow's two cultures not only do not talk to each other, they simply act as if the other doesn't exist.

*

Finally, any discussion of Cyber security must touch upon internet governance. We cannot take security lightly, but it cannot be used as an excuse to limit freedom of expression. Today we see a sort of Huntingtonian clash of civilisations between those countries, mainly authoritarian, that want to censor and restrict the internet and a coalition of democratic nations that stand up for the universal norms of freedom of speech and unhindered spread of ideas. Between those that want an internet ruled by states and one with all relevant stakeholders. This fight will be one of the major international political clashes of the digital age. Alas the recent revelations on surveillance are used as ammunition in an attempt to impose a Westphalian order on the internet following the principle of Cuius regio, eius religio, where religio for us here today is a belief in Freedom of expression and the liberal democratic order. For not so democratic sovereigns, their absence.

Cyber security cannot lie in highly restrictive legislation that plays straight into the hands of

those who have a fundamentally different value system with little regard for human dignity and freedom of speech. Cyber crime and the surveillance scandal are presented as reasons, or excuses, to control and regulate cyber space and to limit the free flow of information. That cannot be the solution. The freedoms we value are equally valid online as well as offline.

Indeed, freedom and security need not contradict each other: secure online interactions, enabled by a secure online identity, is a precondition for full internet freedom.

To conclude, the most effective means to be genuinely secure, to be safe from attacks and surveillance is to go back to the pen, typewriter, paper, and mechanical switch. To give up on mobile phones, iPads, online banking, social media, Google searches, ontime delivery to our supermarkets —everything we have become accustomed to in the modern world. That is one kind of solution. It will not happen.

In short, the more digitized we are, the more vulnerable we are. It is therefore crucial to understand that cyber security is not just a matter of blocking the bad things a cyber attack can do; it is one of protecting all the good things that cyber insecurity can prevent us from doing. Cyber security should not be seen as an additional cost but as an enabler, guarding our entire digital way of life. But we need to do it right. I hope some ideas will come from the panel starting now.