INTRO

I shall start right off saying I am not a geek. I understand basically how the TCP/IP protocol works. I did learn to code at 13, using perfo-tape, some 45 years ago, but all that has given me perhaps is that I am not afraid of computers, that I believe kids can and should learn code as a way to think as well as a foreign language at an early age but that's about it.

What I have spent much time on in the past twenty years is thinking about how to use Information Technology in national development. Initially as a way to overcome the backwardness forced upon my country by thuggish and sluggish Soviet rule. Later, as our computerization policies began to work and we leapfrogged much of the developed, largely Western world, I became concerned with how to deal with the dangers and threats that an IT-based society must come to terms with. This was not simply because my country a mere five years ago was subjected to massive across-the-board DDOS attacks; these were disruptive yes, but in the broader scheme of things relatively primitive.

I have become concerned because it is clear that in my own country as well as many others, IT and the connected life of services has so completely changed our society, that turning back is inconceivable. Yet most of our concerns about cyber threats are military or at best conceived in terms of classical warfare.

Allow me, Ladies and Gentlemen, to explain.

The web and our interconnected way of life represent a dramatically sped-up version of the changes the world underwent in a century of industrialization.

It is a paradigmatic transformation of our world and notions of a nation's size, wealth, and power, where military might, population numbers and GDP relations mean something altogether different than they did a generation ago. Like tag balloons that show trending news, these relations are in a constant flux where old assumptions simply no longer hold; where, a small poor East European country 20 years ago is today a leader in cyber and e-governance, while some large and rich countries remain stuck in the technology of the 20th century.

Where non-state actors can wreak havoc on nation states, where aggression need not even be directed on standing militaries.

MILITARY NO LONGER MAIN TARGET

For indeed, militaries exist to defend a society. In the past to attack a country, to immobilize it one had to attack its military. Today, it is possible to bypass the opponent's military altogether. It can be simply rendered irrelevant, a bystander, as a country's SCADA systems and banks grind to a halt. In the not very distant past if you wanted a nation's wealth you had to take over its mines, oil fields or ports. To do that, you had to fight its military. Today, with a huge portion of wealth generated through intellectual property you need only to suck out their long-generated products from a company's computer system. To impoverish a country you can simply erase their banking records.

Thus, we must put military cybersecurity into context. Defending our militaries against cyber attack does matter. Cyber attacks against military targets are a form of cheap, available force denial.

They allow an inferior adversary to reduce the hardware of the world's greatest fighting force to a nice pile of metal, an F35 or Supercarrier into a piece of legacy technology.

Cyber attacks against civilian targets, however, circumvent military power. Such attacks, either state-directed or freelanced or a combination of the two, go after society, that same society that provide the raison d'etre for a military in the first place. The military of a rich country can spend billions hardening its shell, it can design its own chips, isolate itself from debilitating attacks, but if society itself is reduced to shambles, what is the point of a military? In cyberspace, no country is an island, and no country has two oceans to protect it from conventional foreign threats. Military cyber attacks don't present an existential threat to the functioning of our societies, but civilian threats do. **That's why I am far more concerned about civilian cybersecurity**.

But let us put things into perspective. If we genuinely want to put society at the core of our

security concerns then if you think about it, the best cybersecurity, the most effective means to protect our societies, is to roll back the clock. To forego the advances of the past twenty years, go back to pen, typewriter, paper and the mechanical switch. Give up on mobile phones, iPads, ontime delivery, modern automobiles, electronic banking, Facebook, Google searches, in a word we everything have become used to in the modern world.

In other words we shouldn't care about cyber defence simply because of the bad things a cyber attack can create, but the opportunity cost, the good things cyber insecurity can prevent us from doing. That is to say, we must be concerned because the threats are to our modern way of life.

If we accept then that what we need is defense of the entirety of our societies, a form of total defense, if you will, then we need to re-examine many of the old-style, pre-1990s assumptions with which we approach cyber-security. We must go far beyond, but of course not ignore the military paradigm.

For one, having recognized that that they (whoever they might be) are far more interested in our companies, banking systems (as last weeks Iranian attacks on NY banks demonstrate), and intellectual property, then we have to rethink our government-private sector relations. Especially since the kind of attacks our private sectors are subjected result from a mercantilistic collusion in authoritarian states between the state and its private sectors.

This otherwise old model of political control and collusion between government, business and crime, whether you call it reformed communism, crony capitalism, managed democracy, the Beijing consensus or just plain despotism, has gained a new lease on life in or through cyberspace. We in the liberal democratic West, in countries with low (i.e. good) scores on the Transparency International Corruption Index, have built a solid firewall between the private and public sectors. Even the term Public-Private Partnership attests to the relative separation of the two. No such separation in mercantilistic or authoritarian kleptocratic regimes exists. One serves the other.

We cannot take that route if we want to maintain our liberal democratic order, but we must rethink how the private and public sectors relate to one another, what governments and companies share with each other.

We should take as our starting point that all of what we do in 2012 constitutes our critical information infrastructure. For almost everything depends on a functioning digitized system of one kind or another. One of our concerns, the vulnerability of Critical Infrastructure, CI, our electrical, water or energy production systems are just a subset of our Critical Information Infrastructure, CII. These functions are more important in terms of societal safety and security, but as they are integrated into the larger system that also includes everything else we do that depends on a functioning internet, it is difficult to separate one set of critical functions from another. Thus it makes more sense to look at the whole.

This is what we have done in Estonia. The key is to treat the system as a whole, an eco-system, where at the core lies a secure, verifiable and reliable identification system that ensures that every critical informational transaction can be trusted. This system must also be defensible.

Ladies and Gentlemen,

For the remainder of my speech, I'd like to talk about a certain part of critical information infrastructure, about identity and data. In the U.S., you are tackling these questions through the National Strategy for Trusted Identities in Cyberspace.

In Estonia, the type of ecosystem NSTIC strives to build exists today. The various systems that modify our e-government have been operational for nearly a dozen years and have adoption rates nearing 100%, with more and more services available every year. Estonia has gone further than any other country in the world in investing into digitizing the basic processes of society, within government, between government and citizen and enterprises, between citizens. A quarter of the electorate votes on line, 95% of tax returns are done online, and I really mean online – you log on to the system, the government pre-fills your return from payroll tax stubs and other sources, and you just press accept. A similar percent of prescriptions are filled online. Citizens, as legal owners of their own data have access to their digital medical and indeed dental records. By December of this year, Estonians will have given over 100 million legal digital signatures, and this for a country of 1,3 million.

And securely – in the dozen years our e-government infrastructure has been in use, there has not been a single successful attack on the underlying infrastructure. Even when subjected to massive DDOS attacks that took out newspapers, conventional online banking and government websites, the X-road, as we call our implementation of NSTIC, was robust and remained online and intact.

A way to conceptualize this is that we have a parallel internet for public services, which forms the backbone of our e-government. Technologically powerful, it is conceptually rather simple and hardly unique. It is an enterprise service bus implemented at the level of the entire government and open to participation by the private sector, an opportunity seized for example by our private banks. A system like this will necessarily be at the core of the inevitable move in the future to government cloud-computing.

One crucial conceptual component to a secure system such as the x-road is a rethink of our notions of privacy and identity, the source of most objections to a system employing an ID card. Societies, for some reason especially in the English-speaking world – the UK, US, Canada and Australia seem to have a viceral reaction to any kind of national ID. A nebulous fear of an imagined Big Brother or whatever prevents citizens from adopting a smart-chip based access key that would afford them the secure online transactions.

The rethink we need and which we have managed in Estonia is that the government has become the guarantor of secure transactions online. But the identity is authenticated by a body independent of the government. To illustrate. If I want to retrieve my medical records or make a bank transfer I use my smart chip and a password to establish and authenticate my identity. Once done, I can access say my bank account. The authentification process also certifies that I have reached the right destination, my bank. The bank trusts the authenticator that I am who I say I am and allows the transaction to take place.

The government therefore has stepped in where elsewhere we observe market failure. A bank that builds identity theft and fraud into the cost of doing business is an example of market failure. A power company that treats a cyber-induced power outage as force majeur as if it were an Act of God like a tornado or an earthquake is an example of a market failure. In Estonia, like in many other countries, we have given government new regulatory powers similar to the proposed in the Lieberman legislation that failed to pass Congress. If the private sector is unwilling to take the necessary steps to guarantee the integrity of its online activities we can either live with our vulnerabilities, at our own peril and possible consequences. Or the government must step in to fulfill its most fundamental task: to ensure the security of its citizens. This lies at the heart of the concept of the Lockean social contract, which is the basis of Western liberal democracy.

The success of our e-government system also illustrates the value of treating cybersecurity as an enabler. Our e-government has allowed us to change citizens lives, signing documents with

their mobile phones, never having to stand in line at a government office. The benefits for business and commerce are even greater.

Now think of the new kinds of global commerce this enables:

Last year, 1000 Finnish citizens used their electronic IDs to start businesses in Estonia. This is noteworthy because these Finns could not start businesses online in their own country. Estonia also has a new kind of illegal immigration: we've discovered foreigners who already had the right to live and work in the EU, but separately illegally obtained Estonian residency, in order to gain an Estoinan e-ID, and access to Estonian e-services. And they are flocking toward our freedom- some days ago, Freedom House announced Estonia is again ranked #1 in the world for net freedom.

In Europe, we are now looking at connecting our X-roads and our digital IDs. Ultimately, government data will move across borders as freely as email and Facebook, and follow the international flows of commerce and trade.

Think of what that will mean for us economically:

The public sector in the OECD countries alone constitutes over 13 trillion dollars of GDP. Government, for the most part, has not gone through the incredible cost-savings and streamlinings technology has enabled in the private sector. If we can make that 10% cheaper, that's 1,3 trillion dollars per year. In the EU, we've calculated that building a digital single market is worth 4% of GDP per annum – that's the difference between robust economic growth and a cripling recession.

Again, this is the idea of a high degree of cyber security not as a cost, but as an enabler. Our cybersecurity needs to enable a globalized economy based on free movement of people, goods, services, capital and ideas to flourish.

What should be worrying to this audience, however, is that America is not leading the world in building secure IT infrastructure. I'm not just talking about physical infrastructure, though you

should be worried that the US is 33rd in average download speed, but also about software infrastructure. Estonia shares its IT infrastructure freely – the underlying software is open source and we give it away.

So far, the countries that have approached us for our expertise are in the developing world, those with a wish to leapfrog legacy systems – Brazil, Tunisia, thr Palestinian Authority, Montenegro, Moldova, Azerbaijan, Oman and others have turned to our public and private sector. We are now seeing the rich world catch up – we now have an expert who inside the UK cabinet office advising their IT reform, and several books have been written about our e-ID and x-road in Japan.

My point is not to copy Estonia. There is hardly a need for the U.S. or Europe to do that. Rather, we need to think far more about how to secure and maintain our citizens' digital way of life. To understand where our vulnerabilities are and to move to a more co-operative strategy in all the myriad of areas where military defense is irrelevant. The default option is pen, paper and the Pony Express. Or punch cards and perfo-tape at best, as I did 45 years ago.