Welcome to Estonia, where a month ago we celebrated the twentieth anniversary of our independence, version 2.0.

When Estonia reestablished its sovereignty after a half century of successive thuggish totalitarian foreign occupations by the Soviets, the Nazis and then again the Soviets, we knew we wanted to create a democratic country characterized by rule of law and respect for human rights.

The rules for that were more or less clear. All we had to do was read Charles-Louis Montesquieu, John Locke, Thomas Jefferson and John Stuart Mill. Moreover, there were lots of role models from the preceding two centuries to emulate, plenty of lessons as well on what *not* to do.

After the Soviet period we were also poor. Very poor. So in terms of economic reforms, we also knew what needed to be done: restore the market economy. Here there were many more tried and true models to follow: liberal or what today is called neo-liberal market economy, a more social market or Erhardtian approach, or perhaps a Scandinavian social welfare model. Each had its pluses and minuses. While the electorate has consistently opted for the more liberal approach, it is clear that we would not be charting new ground, rather applying our reading of Hayek or Keynes, Friedman or Samuelson.

The real issue, for me at least, was how sustainable could a country of 1.4 million – roughly the size of the Danish capital Copenhagen – be? Indeed Copenhagen is not an appropriate comparison because a municipal government is free of the requirements of statehood. A city does not need a diplomatic service or embassies, it does not need an army, a navy or a border guard, a healthcare system or a tax authority, a full-time parliament or a supreme court. It need not field troops in Afghanistan, emit its own currency or maintain an Olympic team.

In other words, the requirements of statehood are far greater than mere numerical comparison of population size would suggest. "People have an unbelievable desire to have their own flag, their own currency, their own airline, their own language," said Madeleine Albright in 1995. But the question we faced was whether these desires were sustainable for a nation of our size. In other words, the problem was not being Copenhagen but rather "Getting to Denmark", the successful nation-state as Francis Fukuyama has noted, "where Denmark stands generically for a developed country with well- functioning state institutions. We know what ‘Denmark’ looks like, and something about how the actual Denmark came into being historically. But to what extent is that knowledge transferable to countries as far away historically and culturally from Denmark as Somalia and Moldova?"

And while Denmark had gotten to *us*, invading Estonia in the beginning of the 13th Century and even getting their flag, the *Danebrog*, less than a kilometer from here in 1219 in a battle against us Estonians on what today is the Dome hill of the Old City, we still had a long, long way to get to Denmark.

This briefly encapsulates the real problem faced by a small country struggling to climb out of the ruins of totalitarian rule, poverty and general backwardness. Our fundamental existential question was, can a country as small as we make it?

My own personal answer to this, an answer I would begin pushing and push to this day, came from a reverse reading of a book. The book was *The End of Work,* by American economist Jeremy Rifkin. In that book Rifkin argued that computerization and automatization would lead to massive unemployment and impoverishment because people would no longer have jobs. Computers and machines would do it all for them. The argument was neo-Luddite and neo-Marxist. One example he brings in the book gave me my own *Ahaa* or *Eureka* moment.

Rifkin writes of a steel mill in Kentucky that produced x-amounts of steel with 12 thousand employees. After being bought by a Japanese company and automatized, the plant produced the same amount of steel with only 120 employees.

It was reading that, that convinced me how Estonia had to go. It had to computerize. Completely. For I realized reading Rifkin that actual size does not matter: *functional* size does. If 120 employees, through computerization and automatization were productively equivalent to 12 thousand, then Estonia stood a chance of making it in an increasingly globalized world if and only if we functionally were much larger than our numerical size.

This was how I came on the idea of the Tiger-Leap, the plan to computerize and connect all Estonian schools to the internet, a plan whose implementation I worked out together with then (and again today) minister of Education Jaak Aaviksoo in 1995. In brief, it was not the computerization that was the key but getting people to want to do it. We came up with a government matching program for municipalities interested in investing in computer education. Initially a few were. That great motivator of human behavior, envy, ensured that others followed. For a poor country to achieve four years later complete internet connectivity and computer access for its schools is a story in its own right, but I would rather focus here on the broader picture. The school system is but a small part of the story, essential because you need the nation's youth to be the driver in the process; essential too, because young budding computer whizzes need the proper environment if you want them to produce a Skype, as they did. Today, 98% of Estonians under 35 use the internet regularly and systematically. This, I submit, represents an altogether different population than a generation ago, a population that already demands an altogether different approach from its government.

Yet the school system is just a part of the big picture, which is that Information Technology and its use by the state and government is at the core of Estonia's modernization, one of the most successful modernizations of the past quarter century. ICT, of course, has been the motor of private sector development in the past three decades, and Estonia's Skype is no exception, but the use of ICT in the public sector is where we can genuinely consider Estonia the world's leader. The E-government cabinet, E-health services, online voting, online pre-filled tax returns, e-mobile parking, are all examples of Estonian innovation, but far more importantly, they are examples of the transformative power of intensive and extensive use of Information Technology in the public sector.

II
What we've done…

Before going into what we have developed over the years here I wanted to speak briefly about another pre-condition of an effective e- public services system: inclusiveness. If getting young people computer-literate through putting school systems on line is a no-brainer, at least in retrospect, getting older people and those in rural areas on line can be a tougher nut to crack. Here, serendipitously perhaps, we did it through a public-private partnership with the banks.

Banks realized early that with the spread of electronic banking, branch banking becomes evermore of a cost burden. But how to convince people to bank online?

The government also wanted more people to use the internet for its services. The two sectors, public and private, combined their efforts in an education program "Look at World" (Look@World) designed to teach older people and people living in the countryside how to use computers and the internet. With local schools opening up their classrooms as well as municipal administrations providing public access to computers, we achieved in a fairly short time a computer literate population in segments of the populace that elsewhere have been resistant to technological innovation.

But the real drivers of change have been the services themselves and the changes that underlie a genuine step forward in quality.

Public administration and public services.

The first thing to get right is to understand that the internet is not paper. Simple transference of the logic of paper-based administration to HTML is guaranteed to fail. If you want to create a quality e-service on the web, it is necessary to think of the root goals of data collection and its management and think of how to get necessary information to the user/citizen as quickly and as comfortably as well as securely as possible and to validate this electronically. This applies to virtually all applications.

In other words, E-government is *not* about making it possible for people to fill out the same old forms and questionnaires online, but rather is about achieving the goals of administration and services in the most intelligent and citizen-friendly way using the opportunities offered by IT. For example with the online tax-return, we spare the user time and effort by giving him the information the state already has anyway in the form of a pre-filled tax form that has all the data his employers, banks etc have already provided the tax authorities. The user can check these data, supplement them if necessary but for the average taxpayer, filing a return in this way becomes a matter of five minutes. And it has been so since 1994. 95% of tax returns are filed on line.

I shan’t go into all of the e-solutions Estonia has developed over the years but it is crucial to note the cornerstones, the electronic signature and the decentralized data management system we call the X-road.

The Digital signature is a universal, legally binding method to sign any legal document with notary power, i.e. as if they were signed on paper in the presence of witnesses and certified by a notary. Without the digital signature a public or government service on the web would be taken no more seriously than anonymous internet commentary. It lies at the core of the trust necessary for any genuine services on the web. We've built the critical mass of users since the Digital Signature Law was passed in 2000, first with chip-based smart cards and card readers and later with mobile phone-based applications and implementations. The open design of the system helps any new public or private application to build on top of the existing trust between citizens and the state, and allows the surrounding technologies to evolve over time, and not become an incompatible legacy system to deal with as every new technological generation takes over.

X-Road is the backbone of e-Estonia, the invisible yet crucial link between the nation's various e-services databases, both in the public and private sector. Our databases are decentralized: there is no single owner or controller, every government agency or business can choose the product that's right for them and new services can be added one at a time as they become available. X-Road has evolved from a system used merely for making queries to these different databases into a tool that can also write to multiple databases, transmit large data sets and perform searches across several databases. It is what has allowed us successfully to implement the digital health record and the digital prescription, of which more later. Similar attemptsÂ using stand-alone digital prescription and healthcare record systems have failed precisely because they have been stand-alone. Currently more than 100 organizations have joined the X-Road.

With a universal and open foundation we have created new services and products, most notably:

Internet voting or e-elections, is a system that allows voters to cast their ballots from any internet-connected computer, anywhere in the world. Unrelated to the electronic voting systems used elsewhere, which involve costly and often problematic machinery, the Estonian solution is simple, elegant and secure. During a designated pre-voting period, the voter logs onto the system using an ID card or Mobile ID, and casts a ballot. The voter's identity is removed from the ballot before it reaches the National Electoral Commission for counting, thereby ensuring anonymity. In 2005, Estonia became the first country in the world to hold nation-wide elections using this method, and in 2007, it made headlines as the first country to use i-voting in parliamentary elections. In 2011, 24.3 percent of voters cast their ballots in this way.

The E-police system is based on the principle that providing the best possible communication and coordination will lead to the most effective policing. It involves two main tools: a mobile workstation installed in each patrol car, and a positioning system that shows headquarters each officers' location and status. From a glimpse of a passing license plate, officers have immediate access to data on the driving license, vehicle, owner/user and technical inspection information, insurance policies, basic data on the person such as place of residence, photograph and telephone number, etc. The system is integrated with the Schengen Zone's information system, allowing them to see if the vehicle is stolen or if the driver is wanted in another country. These queries used to be handled over the radio and typically took 15 to 20 minutes, now they take as little as 2 seconds. The difference allows officers more time to answer calls, resulting in more effective policing.

The State Portal, eesti.ee, is a one-stop-shop for the hundreds of e-services offered by various government institutions: rather than having to hunt for a particular service on the Internet, users (citizens, entrepreneurs, officials) can simply head to this gateway site and find the appropriate link. Once logged into the system with an electronic ID, the user does not have to repeat the log-in when accessing each different service.

The key, however, remains getting the fundamentals right. You need a flexible and decentralized system and you need a legal signature with the attendant hardware and software. One visiting delegation, impressed with e-elections wanted to rapidly implement it in their country but asked, "please, tell us how we can do it without the ID card." The point is, you can’t. If you want a safe and secure and user and citizen-friendly e-country, there are no shortcuts. Without the foundations it will fall apart or more likely, never get off the ground in the first place.

An additional and crucial element we have discovered is **Citizen education**. An information society requires, in addition to intelligent e-administration, an informed user, a smart citizen who is capable of making choices. Responsibility for privacy protection for example, rests much more on the citizen than earlier. If before, with paper administration and services one went to speak to an official whose task is to offer advice, warn of dangers, ask for identification and verify one's identity, then in e-administration, e-government the citizen himself is responsible that his e-ID card is in his possession, he is responsible to read and be aware of the consequences of his e-choices. In the e-health portal, he or she decides who is allowed to read his health records, etc. This is a new kind of relationship, where empowerment through the internet also carries with it new responsibilities.

III

ICT public sector and the future. When discussing development in post-communist countries, I like to paraphrase the opening sentence of Lev Tolstoy's *Anna Karenina*: All successful countries have reformed alike; all unsuccessful countries find their own excuse.

I believe that when it comes to ICT and the public sector we will go beyond the restriction of "post-communist": Successful governments will have implemented broad e-services solutions, unsuccessful governments will have failed to do so.

Rather than look in the final part of my talk at specific ICT public sector solutions I would look at broader general issues we all face, be it in Denmark or the developing world.

Openness and democracy. Absence of transparency breeds corruption. E-tenders, publication of expenses, public sector incomes on-line all open the governing process to inspection. This is fairly elemental. Perhaps less obvious but no less important is that e-governance allows us to eliminate nodes of opaque discretionary and arbitrary decision-making. Which in plainer language means that administrative decisions that in reality are non-discretionary – applications of all sorts for example – can be done online, without anyone arbitrarily having a say in the matter. More bluntly, you can't bribe a computer, no online system can say, I'll process this for a fee. In fact the best argument for use of ICT in government and the public sector more broadly is the cleansing effect it has. Today in Estonia, corruption remains in those areas, primarily municipal government-related, that have resisted ICT-based transparency rules regarding permits and tenders. I believe that Estonia consistently ranking as the most uncorrupt at the national level of once communist countries is directly a function of this transparency.

Demographic shrinkage, aging and health: E-health: ICT means not just better healthcare but leads the way in transforming the doctor/patient relationship as it has developed since Hippocrates. No longer is it a priest/supplicant relationship. ICT allows, indeed forces a revision of the relationship to where the patient is finally the owner of his own health data, open, at his own discretion, to others, including other doctors, which brings in a new dimension of transparency, oversight, easily obtained second, third or more medical opinions and indeed genuine competition, which can only lead to better quality healthcare.

One of the growing concerns of Europe, Estonia's own concern of its smallness writ large, is our continent‘s demographic decline and our top-heavy demographic pyramid. We have fewer and fewer children, which in turn means ever fewer future workers to pay the taxes and bear the costs of a burgeoning aged population. In addition to forcing Europeans to look evermore toward e-solutions in general, a shrinking work force and growing pensioner population will require completely new approaches to health care.

Currently I chair the European Commission Task-Force on e-Health, comprising experts from technology, law, medicine, patients rights organizations, tasked with laying out a future European policy of ICT based health. Some solutions are simply logical extensions to a European level of what we already have operating in Estonia today: Healthcare records accessible all over Europe with automatic translation so that a Valetta hospital treating a Finn who falls ill in Malta can access his Helsinki cardiologist‘s observations. Or that a Spaniard in Tallinn can refill his digital prescription from his doctor in Toledo. This, as I said means simply expanding existing national programs all over the Union.

More challenging is the demographic/retiree/quality aging problem. It is clear that current approaches to healthcare are unsustainable both in terms of cost as well as personnel. E-Health solutions that allow people to have their health be monitored at home and not in the hospital, where sensors can pick up dangerous changes in blood pressure, heart rates, even insulin levels long before patients themselves begin to feel anything, all can lead to improvements in the quality of life as well as extend our lifespan.

This is the positive side of moving forward on e-health. We can live longer and better and do it at less cost. The negative side is that *not* moving on e-health means an increasing aged population will place ever greater health care burdens in both cost and man-power on a working population decreasing in size and hence with decreasing tax contributions.

Big Brother (x-road/flagging). Generally, peoples‘ fear and hesitancy regarding greater computerization comes from a George Orwell/1984-based metaphor of a single computer or data base where all your information is stored, knows everything about you and can use this information at will and for evil purposes. Indeed, this kind of fear is understandable and continues to permeate discussions of social networks such as Facebook, the use of cookies in web-pages, etc… so I wouldn’t want to belittle it. And as Evgeni Morozov has described in his book *The Net Delusion*, social networks themselves can be abused by totalitarian and authoritarian governments in rather Orwellian ways. Indeed Social Networks' use and sale of private data from unwitting postings will be, I predict, an issue of increasing concern and most likely regulation in the future.

The decentralized, citizen-owned data bases of the X-road developed in Estonia and analogous systems currently under study elsewhere stand in stark opposition to the Orwellian model, though the fears associated with government data bases appear to be universal. We have implemented safeguards to guarantee any unauthorized access to data will be caught. Every time a person's data is accessed it is recorded automatically. Those lacking authorization are automatically flagged. Let's face it, people will try to pry but electronic data are far better protected. A police officer snooping in her boyfriend's records will be caught when doing so in an electronic data base; no such records or flagging would take place if we were still in the days of paper files. Decentralization and strong watchdog controls, flagging etc, I believe remains at the core of user acceptance and trust of any government or public service data base.

In short, in order to be competitive, societies and countries need to be able to rely on ICT. But for democratic societies to tolerate and go along with these processes, ICT solutions A) must be decentralized B) a citizen's data must legally belong to him or her, with complete access to all of one's data a *sine qua non*, and C) access to others must be strictly isolated, i.e. accessible only to those with a legal right to do so, which implies strict monitoring of those accessing others‘ data combined with strict penalties for those who violate the privacy of a citizen's data.

Security. Finally, let me speak about something that looms large in any discussion of e-services, ICT use in the government and in public services: security, cyber attacks, malware, hacking etc… Especially since the more we rely on Information Technology in our daily lives and to run governments, the more vulnerable we are, as we in Estonia discovered with the massive DDOS attacks on our public and private ICT infrastructure in 2007.

Cyber-security is today's growth field, with no better testimonial than the fact that both NATO's Cooperative Cyber Defense Center and the European Union's Home and Justice affairs data centre are located here in Tallinn.

Yet I would argue that this is an area where we cannot isolate the government from the private sector. Indeed, we need to realize that our vulnerabilities in government and the public sector are intertwined with vulnerabilities in the private sector. All the more so since attacks on our government systems as well as our private sector are themselves produced by new "public-private partnerships" where mafia or other groups contract themselves out to, or work hand in hand with governments to attack, hack, steal and disrupt.

Slowly, it is, moreover, dawning on us that cyberwar does not have to hit state or civilian infrastructure, but rather our economies, through piracy, that in fact perhaps we are too fixated on the militarization of cyber rather than state-sponsored theft.

For technologically advanced countries, including my own, with Tallinn as the R&D center of our flagship company Skype, it is the theft of intellectual property that can in fact cripple or at least severely wound our economies. Let’s be sure about this: much of what makes modern economies function and prosper is the product of huge R&D investments, both public and private. The EU has set a goal for its member states to invest 3% of GDP in R&D, a goal few meet but then again few meet the NATO goal of defense expenditure of 2% of GDP. Much of the democratic West’s primacy rests on innovation, on new designs, pharmaceutical products, software solutions etc.

A company that invests hundreds of millions or even billions of dollars or euros in new products can see it all evaporate if the research is stolen: the value of the product comes from those years of creative work and dollars invested in developing it. Yet it can all be stolen. At which point someone else somewhere else has gotten for free what your country’s best and brightest spent years to develop. You lose the tax revenue, someone else reaps the profits.

This is piracy. Pure and simple. And it is as dangerous and threatening for modern states as piracy in its more primitive forms off the Barbary Coast was at the beginning of the 19th Century or in fact today off the coast of Somalia.

As is the case with classical, marine piracy, intellectual property piracy is not only a threat to our economies, it is also a threat that falls into the category of PPP or Public-Private Partnership, where state actors condone or turn a blind eye to it, if it benefits their economies, or even explicitly use it just as it was to the Barbary States under Ottoman rule. And as with the Barbary pirates, cyber attacks against our companies can be met head on only with cooperative and concerted state action.

Today the Public-Private Partnership paradigm that we see in both militarized cyberwarfare of the Botnet type as well as in the systematic theft of our companies’ intellectual property should give us pause to rethink our own relations with the private sector. I recently shared a talk and panel discussion with Swedish Foreign Minister Carl Bildt on cyber security at the Royal Defense University in Stockholm where, during the Q&A, the head of cyber security for Ericsson stood up and asked point blank: "Why are you (government people) not sharing with us? *We* ar e attacked just as much as you and probably more."

I can’t say who is attacked more but he made his point and in fact made me rethink my views on cyber-security. A few weeks later I asked the then head of cyber-security for the British MOD, Dame Pauline Neville-Jones, why the UK had suddenly, after a number of years, taken such an outspoken position on the need to work jointly on cyber defense. Her answer was more or less the same: our companies are coming under massive attack.

What I suspect, although I can’t at this time say how, is that we will in the future have to rethink government-private sector relations. We in the liberal democratic West, in countries with low scores on 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 in the normal scheme of things. No such separation in mercantilistic or authoritarian kleptocratic regimes exists. One serves the other.

Yet if the basis of our relative economic success, our private sector, is coming under attack from state actors, we need to come up with new ways of talking to, and sharing with, the private sector. This of course runs against the grain of how we have been doing things. Yet we need to address the problem.

As I see it, there are two issues. One, we need to come up with new ways to talk to the private sector. Security clearances, sharing of sensitive information – in both directions from government to private sector and vice versa needs to be made far less ad hoc, far more based on rules that would allow us a greater deal of flexibility to face new threats without at the same time allowing the crony-capitalism that destroys democracies.

Secondly, however, we on the state-side of things need the brains that go to the private side of ICT. Let’s be honest, Estonia can’t pay for the genius software developer at Skype. But then again the U.S. Department of Defense most likely is not able to hire the top guns at Apple, Microsoft or Google *either*. The other side(s) can. Back during the Manhattan project the U.S. could hire Edward Teller or Robert Oppenheimer for a professor’s salary. But nuclear physicists could only work for a university or for the government. Today neither the university nor the government can afford the modern cyber equivalents of an Edward Teller.

All this puts governments at a disadvantage in developing cyber defense. We cannot necessarily afford the best and the brightest. Here in Estonia, however, we have developed one solution to this problem, the cyber-defense league, which we can translate, depending on your own national version as the cyber home guard or the cyber national guard. These are weekend warriors with pony-tails, computer geeks who have high-paying day jobs running IT departments, working software companies, banks etc. who find it cool to volunteer for their country. We offer them the opportunity to help with our defense. Not running around the woods in camouflage suits but building our cyber-defense capability.

Today we have about 150 volunteer computer experts in the Cyber Defense League, not a bad number for a country with a military of 4000. They are motivated and patriotic, and let’s be honest, it’s sexy to work on these things.

We are only starting out but I mention this initiative as the kind of creative solution that we need to begin to consider to be able to guarantee the highly sophisticated e-services and the high R&D driven companies a modern society depends upon. When threats are no longer classic threats, our responses can no longer be classic either. At least if we want to maintain the upper hand.

In closing, I must admit that I have no doubt raised far more issues here than I answered. Rather, my intent was to point out in broad brushstrokes how different the world of the public and government sector has become with ICT. We have wonderful new tools to solve old problems. We can develop innovative solutions that improve the lives of millions. And we have discovered too, some decidedly un-wonderful threats and new problems.

Estonia’s experience in the past twenty years reflects this: we became pioneers in use of ICT in government first because it seemed the best if not only way to leapfrog decades of backwardness caused by awful Soviet rule; Information technology and its use in the public sector as well as the private became the engine of our rapid development, and enabled us to become a leader offering innovative solutions we gladly share with others. And almost as if on cue, we also became the world’s first victim of purposive, directed, massive attacks against a nation’s public ICT infrastructure. And, thence one of the world’s centers of cyber defense and security.

Nonetheless, we are e-believers. We are proud of being pioneers in e-government. And we are convinced that a public sector ICT approach that is citizen-centered, secure and transparent is the future of good governance in the 21st century.