Well, thank you very much. I start off with a two-finger comment on **Joe Nye** which is just that there is an article in Politico last week about the Russians making an offer to the U.S. on a bilateral treaty which the U.S. rejected. Of course, as a European I would say, yes of course the Russians who have clearly meddled in Germany, the U.K., Spain, Italy, the world agency or World Anti-Doping Agency that it does not really encourage us if there is a bilateral treaty. And we are left out to continue manipulation. But basically the U.S. rejected it because it is kind of asymmetric, because you already know the result of the election. So I mean what's meddling going to do.

Anyway, get to my talk. I am going to start talking about security from a ground up level because I actually think and expand upon that security, as at least in all post enlightenment democracies based its approach on John Locke's model that the individual gives up his Hobbes' right to kill someone else to the state in return for security, be at your local police, your national security agencies, or internationally, in the Army. And what we have done in Estonia is actually put the state at the center of the security. At the same time, just let you think we are kind of **deal with it**, European governments were probably far less intrusive in people's lives than in the United States. But more broadly I think that we have to rethink of it.

Most aspects of our lives, in looking at living in the digital age basically ever since William Gibson and his dystopian novel "Necromancer," took Norbert Wiener's term "cybernetics" and popularized the prefix "cyber." This prefix is proliferated to almost all spheres of human activity which I think is an indication of how much the digital world has permeated our lives. So we have cyberpunk, cyber crime, cyber hygiene, cyber space, cyber Pearl Harbor, cyber war, cyber security and of course inevitably cyber sex. Rather than be mown as some have the ubiquitous use of the prefix, saying it is meaningless, I actually welcome the ubiquity to emphasize how profoundly our lives and our societies, our nations and indeed almost all human endeavors have come to be depended upon digital communication.

So basically we **are into** the privacy of emails or our electoral democracy, to our infrastructure, right in apartment sharing, the integrity of our financial system, banking, the ads that we see on social media during electoral campaigns. All of these are subject to manipulation and attack. All of these, with the exception of social media and the sharing economy, also existed before the

digital era but they now have all been altered by the free movement of electrons and are in completely different form, which requires us to rethink much of how we do things in all other aspects and realms of human activity.

And this is of course all due to the the increasing power of the silicon chip or so known as Moore's Law which still doubles every year and half even if it's slowing down a bit because we are pushing the limits of physics. But basically the world is nonetheless completely different from the way it was 25 years ago.

While the all things digital have changed beyond belief, government's policies, laws, regulations actually have failed to keep up with this. (Of course we will talk about what the government can do on cybersecurity, cyber governance is. That is very good but on the other hand we actually have not looked at all the rest of life.

We have events such as when 145 five million adults in the United States had all of their financial records stolen. I mean that is probably 80 percent of the adult population. It was completely untouched by government regulation except for the fact probably from sort of old style rules that the management sold their stocks before informing the population that their data had been stolen. We have to come to terms that this is a much broader issue.

And I guess most importantly if we look at the core of our digital security and I'm not talking about the government, the NSA and our electrical infrastructure, but basically what we, all of us, do online started out 35 years ago with a system that worked fine then when there were about 3,500 academics using a network called BitNet where security relied on an email address almost always ending with a top level domain of dot edu. These people generally did not pose a security or criminal threat. Yet today there are 4.2 billion people online. We fear all of these things such as cyber war, cyber crime, docs, emails. But basically what we are dealing with is that since we use BitNet we have had 22 or 23 iterations of Moore's Law, which means that today computers are 8.4 million times more powerful than they were when we started using this system among 3,500 academics. We also have an increase of a roughly the same order of magnitude from 3.5 thousand people using BitNet to 3.5 to 4.2, depending who you ask, billion people online.

We've been very slow to realize this. Say, **Joe Nye** pointed out in an article 6 years ago, immediately after the Munich Security Conference without naming me, he quoted me, that this is the first time Munich security conference has ever dealt with the issue of cyber security. That was 2011. Up 2011 till the Munich Security Conference, the premier conference on security of the world, had not even a single panel on the issue of cyber security. Now, of course, the Munich Security Conference has an entire separate conference of cyber security. But that just shows how recently this was not considered an issue.

Now what I will try to do today is to try to look at cyber security at three levels, beginning with the individual and then moving on to the state and then finally getting to the international level.

And again to reiterate, my point of view is that security has been the responsibility of the state pre-digital and it remains so today but the state has failed to keep up in general in most places and that this does remain a key aspect of John Locke in the Social Contract where we do give up certain rights in exchange for protection against sort of Hobbes's War of All against All. We have also gotten there in the analog or physical world but we are very slow to get there in the digital world.

Ultimately I would argue that security is a political choice based on policies, laws and driving from those laws and regulations, just as we have in the physical and analog world civilian control of the military as a core concept in democracies, Habeas corpus laws regulating use of guns. Again when we get to digital we are fairly poor in this respect.

When we come to cyber world, I argue, we are too focused on the technology rather than the policies, laws, and regulations.

I would say, specially now knowing the system we have created in Estonia, that actually the technology is not that advanced but we are way ahead of everyone else when it comes to use of digital technology. This is a function of the laws. I should mention here that just this week in The New Yorker you will be able to read probably the best article I have ever read and I think I have read every single English language article that has ever come out on my country and digitization but the best article that has appeared just came out yesterday it's in this week's New Yorker it's

written by a guy named Nathan Heller. That describes the way everything works in a very nice way so I do not even get into that.

One thing I should add before I talk about what we do. There is a huge difference in this regard between what we and most countries do. Because our focus has been always on the gee whiz aspects of technology which became clear to me when after 25 years of dealing with digitizing my country. I mean aside the fact that I was a geek once but it is always tough going politically. When I finally finished my term, my dream came true. I was invited to Stanford, the Mecca of innovation in IT. Of course that is where everything is. In a ten mile radius of my office I have the headquarters of Apple, Google, Facebook, Tesla... I mean you keep going on and on. I guess only Microsoft is really missing. And on top of that three miles away from me is Sand Hill Road which basically funds all of this enormous innovation.

When I went to register my daughter to go to school, I had to bring electricity bill to prove that I live there. Then after she had to take an E.S.L. exam because she was going to school in Estonia and she placed out of taking a catch up course and she had to get permission to enter a regular English class. So I had to sign two pieces of paper. I had to deliver one to the school, physically signed paper, and the other one four miles away at the Municipal School District headquarters. When I got there, there was a line of about 20 people. I said I just have piece of paper to drop off here and the last person said we all just have a paper to drop off here but they have to make a photocopy of it. Then suddenly it struck me that in fact everything that I had been experienced in that process, except for the photocopying, was identical to the 1950s. Nothing it had changed, except in the 1960s you started getting photo with Xerox machines in the U.S. school system, so you could actually make a photocopy. I got to say that to illustrate where we are in most countries when it comes to digitization.

We took a different route. I want to by the way mention what it is like to register a car. It usually takes one to two days sometimes three. Unless you buy a new car and the dealership does it for you which I had to finally end up doing.

But what we did in Estonia, just for background, I mean why we did, what you did, which I mean we emerged out of the miasma of the Soviet Union in 1991 or reemerged because we had been independent. In 1938, the last full year before World War, Estonia, and our linguistic

cousins across the bay, or the Gulf, had the same GDP per capita. When we became independent again the difference between GDP per capita between our two countries was 13 fold. We were still basically operating with no infrastructure except for military infrastructure; all roads that were built during this Soviet period were for military purposes. So looking at this awful situation, people came up with all kinds of plans. I proposed (since I had been talked in a real fluke and serendipitous event, I learned to program at age 14) why don't we teach kids how to use computers. We embarked upon in 1995-1996 that by 1998-1999 we had all schools online.

Schools had labs which we opened to the public after school hours so that other people could learn to use computers. Keep in mind everyone is poor so they cannot buy computers but they do have access to them. By this time we had gotten this sort of thinking that maybe digitization really is the way to go for the for the country. But we realized somewhere around the late 90s that we could do it differently because ultimately we were worried even then about security and what that meant and we do have a neighbor next to us that is very big and probably very good at causing problems in the digital realm as the US has discovered later on.

So we thought long and hard about what it is that we need to do. One of the things we came to very quickly was the fundamental issue of cyber security for the population is identity. Who are you? We all know the old New Yorker cartoon "On the Internet, no one knows you are a dog,". Actually, the fundamental problem of cyber security is that you do not know who you are talking to, (in fact this is where differs from what I will talk about later on the kinetic world of warfare), you don't even know if he is in your own country that you are talking to who you are talking to.

So what we realized is that we must start off with a strong digital identity and this is what one of the key axioms I would argue for the future of digital security.

Of course that sounds good theoretically. What that meant in policy terms was that in 2001 we offered everyone living in Estonia at that time citizens' permanent residence a unique chip based digital identity card, in that communication was insured with two factor authentication with N2N encryption.

And I said we did this because we realized even then that the primary model of e-mail address plus password is not going to last for long. In fact, today there is no password that cannot be

broken in the email plus password paranoia through brute force hacking. If you do not have two factor authentication, you might as well give up and this already means that on most transactions that you do in life in most countries, you cannot be sure of anything.

We did this with a chip card plus a code. I am sure that people are really interested in this. We see in many places today two factor authentication is slowly coming in. Apple also uses it as Google. **The problem with two factor authentication is the ways that in most places.** For example, at Stanford that has become the norm because of a big hack several years ago.
The **S7** protocol which governs the communication between mobile phone communications has been hacked, is hackable. In fact the first case of a big hack was the loss of 3 million euros by a German bank this Spring that did use two factor authentication using a mobile phone second factor.

So that was how we started off. We did this on a public-private partnership basis because every interaction has to be authenticated. The verification or certification of each transaction is done by a 50-50 public-private partnership, half paid for by the government, half by a consortium of banks.

The second step was that using a two factor authentication with a highly encrypted public key infrastructure. Encryption meant that we could offer all people living in the country genuine security, or starting from the premise that nothing is complete secure, at least far more secure than the kind of security the most people enjoy in most places.

We have been using until then we found out that the that **infinity** and produced a **full flawed chip, or 2048,** we did it fast. I guess unlike most companies in most countries, we actually said we had a problem with the chip. And now we have gone over from our say to an elliptical encryption. As I say that other countries that use the same chip unfortunately have not been very open about it as we were.

Going back to 2001, we did one more step which is actually a key to make creating a functioning digital society in which again most places have not undertaken at all which is that we gave the identity legal efficacy. You can sign legal documents online with this system. That means hooking it up to a national registry. This causes howls of indignation from the Five

Eyes countries, also the Anglosphere, the U.K., Canada, the United States, New Zealand Australia, who say we will never have a digital identity, let alone any kind of legal efficacy, which I would find kind of odd because in fact the United States, the U.K., Canada etc all offer passports in which the state says you are you. All we're doing is saying, the state is saying, you are you to enable legal transactions.

Digitally, as opposed to having it in a physical passport, the use of our system and I mean the card in here as a behavioral economics is that we make it mandatory to have a card. You never have to use it but you must have one. Why do we do that? Because uptake rates of digital identities in most countries, or today in Europe, all countries must issue or offer digital identity, the uptake rates are 15 to 25 percent.

The early adopters are the ones who take out a card. We decided we would make it mandatory because no services will develop either in the public sector where different ministries should be developing things or in the private sector which would have an interest in this. They would not do it if they think that 85 percent of the population cannot even use this service. So we have things such as digital prescriptions which are used actually today by 99 percent of the population. You do not ever have a paper prescription; you call your doctor and he will renew your prescription or your doctor writes it in when you go see him. No one takes the effort to develop those kinds of systems unless you have the private sector and the public sector assure that basically everyone can use this.

So this is laying the groundwork for digital society and of course what makes our bank transactions secure instead of what I find here is that it is all card based chip, be it up for mobile phone or your card. We do not have checks in Estonia. I read recently how one system works here is that you can you have electronic banking so you go online, you do something and the bank prints a paper check and then mails it. This is not a digital society, I would argue.

Basically, the state guarantees ID and it seems to be the main stumbling block in most countries for a secure digital society. My argument is this is simply something in a democratic society that if it is responsible for the security of the citizens, it must offer this. I mean you may not want to

go the full step that we did, that you make it mandatory, then you basically assume that digital services, at least on the part of the government, will not take off.

I just read last night a perfect example of why a democratic government that wants input from its citizens needs a digital identity in the ongoing debate on net neutrality. The FCC, like many federal agencies, asked people's opinion and got a million fake or bizarre nonexistent comments.

Against net neutrality, I don't know how many got in favor of maintaining that neutrality. But unless you can log on and be you as a citizen of the United States commenting on impending regulations then what's the point of asking anyone. In fact, some four hundred thousand of the comments came from Russia. I mean this is not how you run a democracy or at least this is not how you do open government soliciting opinions from your citizens. We have the same system in our country where, on various issues, we ask people's opinion. But you have to do it by saying who you are. If you do not say who you are, there is no point. I do not want to get into issues of anonymity and how crucial that is or may not be and how it would may be ultimately a victim of our lack of cyber security in the cyber realm. Nonetheless I would say that without a secure identity, the functioning of a democracy becomes, I would maintain, stymied.

The second thing we did (just to talk about how we have put security into the system) is designing a very different architecture from what is usually used. Most big countries or most governments have used centralized databases. The OPM hack: 15 million or 23 million U.S. federal government employees including CIA, NSA personnel, including their personal psychological profiles were hacked, as you probably know, two years ago. Does it matter who did it? The fact is that they had all of this stuff easily accessible and in clear text that was not even encrypted. I would find again unconscionable not to mention the kind of hack we saw with Equifax.

What we realized quickly is that we could not have a centralized central database for purely economic reasons. In the late 90s everyone was going after big central servers. We were sort of where we were. We had what we had done: every ministry, every agency, every company had its own servers, often using different systems and also with a great degree of independence, but at least arrogance, there were little fiefdoms. So in trying to figure this problem out, we had some mathematicians of ours came out with a distributed data exchange layer which we call X-road, in

which everything is connected to everything through the authentication of your identity. Basically, the idea is that if your identity gives you the wall and the moat of a castle. Once you breach the moat and the wall, you are in and everything is open to you. In our system, if you breach the moat and the wall you are still stuck in a room: one room, one person. You can get something for that one person but you cannot get the rest of citizens.

I would like to play a three-minute video just to give my throat a break and as a little commercial to show how our system works.

"Running a modern state is a data centered endeavor. Ensuring the functioning of the state requires administering very large quantities of data. Estonia lacks a centralized or master database. Data is stored where it is created. Each agency administers its own data separately and data is not duplicated. At the same time state authorities and agencies need data outside their per views in order to function. For example, the police constantly require information from the population registers. Likewise, the unemployment insurance fund depends on information from the health information system. How can authorities securely exchange important data? First the data must be easily accessible by the authorities that are authorized to use it. Second the integrity of the data must be maintained: no third party should be able to make any changes to the data while it is in transit. Third the data must remain confidential during its journey: it must be protected from the eyes of unauthorized parties.

The X-road is a data exchange platform that fulfills all three of these requirements. The X- road makes life simpler for both the state and for the citizens. For example, when a child is born, information about the birth is sent directly from the hospital to the population register. From there it is sent automatically to the health insurance fund so that the child will have health insurance and a family physician. This prevents the creation of excessive paperwork and saves time. The state functions in the background. The X-road helps authorities make work processes more convenient. Many activities can be automated which frees employees to deal with matters that require human involvement. Authorities also do not have to worry about the authenticity of data. They can be confident that data received from the Tax Board definitely originated from the actual tax board. Additionally, the X-road can be used regardless of what technology and authority use this. For the state, the X-road, above all, makes it possible for authorities to

efficiently exchange data among themselves. Sensitive information moves securely and the system itself is so resilient that it cannot be easily brought down by those with malicious intentions.

Since the birth of X-road in 2000, the system has operated continuously without interruption. The X-road helps the state see the big picture of how different authorities are connected to one another. In addition, the X-road makes it possible to exchange data not only within the country but also across national borders. That is, of course, if databases and information systems are working properly. The biggest beneficiaries of the X-road are of course the citizens. They enjoy the benefits of a better functioning state and save all of the time they would otherwise spend on submitting papers and forms. How much time? During the time it took you to watch this animation, the X-road saved around 240 working hours in Estonia. Cool"?

Now what this does, among other things, is, in addition to giving you security, it changes the nature of bureaucracy for the first time since it was invented 5 thousand years ago, either in Mesopotamia or China.

Bureaucracy has always been the serial process. If you want the permission to do something, you apply with a piece of paper. The paper goes through one agency to another agency. Think about establishing a business, you have to check if all the board members pay their taxes, someone else check if they pay their alimony, someone else has to check if anyone has ever gone bankrupt. So it just takes quite a long time. This makes a bureaucratic processing parallel. In fact, which beats things up from establishing a business in my country is it takes about fifty minutes because all of those queries are answered simultaneously.

This system also allows for greater transparency and reduction of corruption because basically decisions are made by checking the boxes rather than by having an official who uses his discretion to decide whether you get something that you are entitled to or not. If I want permission to dig hole, I have to apply to my municipality just to make sure there is no water main down there or there is no electrical cable. In a lot of countries if you apply, you know you should get the permission but there is an official there saying "well you will not get it for free". That is, you have to pay in whatever currency.

These kinds of decisions are made automatically. The best result however of this is we have applied a once-only rule, which means that the government not ask you for any information it already has. I mean once you are identified, you no longer have to write your address down again, your telephone number or any of that stuff because this is ALL done online.

And the system has now been adopted from us (we give it away as foreign aid) by a number of countries. This platform is kind of foreign aid on a thumb drive. Finland, probably most prominently, with us now are jointly developing its own open source non-proprietary software. Mexico is adopting it; Panama is taking over; Moldova has had it for a while; Georgia. Countries vary in how much they do this. Oman. We gave it to the Palestinian Authority but they never use it. So it really depends.

But again what this does allow us, from the point of view of the citizen, is to go do things that traditionally have not happened at all. We will as of next year have cross-border interoperability of digital prescriptions so as Finns are coming to Estonia. We get too good a time, we get eight million Finns in a year. If he loses medicine, he can then call or write his doctor in north of the Arctic Circle. The doctor will then remove his prescription. He will take his Finnish ID, plug it into any pharmacy, put in his identifying numbers and he will get his medicine. I proposed this 5 years ago to the Finnish President and next year will be six years since I proposed it. That is how long it takes the technology would probably, as in most cases, take about three days to do all this. Political will, policies, laws and regulations have just taken that long to go anywhere.

Further on digital security and security before I move on to the big picture, the big issue in Europe has, especially since Snowden, been privacy. As privacy is, of course, very important, I would argue this system allows far more privacy than the current system but does require a certain degree of trust which is why we do not have backdoors. If you had backdoors you would no longer have trust and no one uses the system.

But the real issue to my mind has been is really data integrity.

I may not like it if someone publishes my bank account or my blood type. If someone changes my blood type or the record of my blood type or someone changes my bank account number or contents, that is a disaster. So what we have done is to put all critical citizen data, health records,

property records, law cases (because now they are all digital and you would not want those changed) on the block chain.

It is interesting that all public sector is in all our private block chain because as if the public want to take forever to work as with Bitcoin but it's on a private block chain and administered by the government, which then means that you cannot change these data.

The other thing that we have done for security in addition to all of this is that as a small nation that has been invaded about 20 times in the last thousand years, we do worry about our data. Based on the experience of Japan which lost about five percent of its of data in the Fukushima incident, we have now established a data embassy. Applying the Vienna Convention on extraterritoriality of diplomatic representations, we have given our big server diplomatic status. It is in Luxembourg and there will be others so that if we happen to have (I mean we will not have) any bad seismic events most likely, or if I were Greece, I would certainly do something similar. Not a happy place for seismic events but certainly you want to keep your data elsewhere. It is not an issue for the United States. The U.S. is huge and generally has not to worry about all you need or keep your data in several different places but for smaller countries, you probably do need to think about these things.

And the final thing and at the national level of what we do is that we have a prohibition of un-updated software. All you have to do is look at want-to-cry which took down the UK's entire national health service because the UK being too cheap, did not update. For the version of Windows they were using, Microsoft stopped updating in 2009. The UK and Microsoft then made a special deal to keep it up till 2013 but even that time lapsed and then this spring 2017 you had the want-to-cry ransomware which shut down the medical system of a big European country.

We cannot allow that. This is again, I think, a fundamental issue that needs to be dealt with both in the private and the public sector. You cannot have legacy software. In other words, you must think of software as an operating cost, a running cost. Most companies and most countries think of software as a capital investment, right? It is not like a car. It is not as if you bought a car two years ago, you do not need another one for three. You must always keep your software up to date. Or as in the Equifax case when they identified of a vulnerability in February, they did not bother patching it until after they were breached.

I mean if you are not going to get companies to observe that and if governments do not observe that, you are going to have to legislate that.

Certainly, in the case of Europe, the application of the new general data protection regulation will force U.S. companies at least in Europe to worry about patching things or what happens to citizens data because the fine is going to be four percent of a company's revenue worldwide, which is no small thing. People may complain and moan about the regulations of the European Union but personally, I think, after Equifax, there's nothing you can say about that. I am more surprised that there has been so little of a citizen outcry on all of this. I am also surprised that all kinds of things such as what happens to data in this country or in a number of European countries and its use, for example, Cambridge's analytic use of data is brought in creating highly targeted, highly granular ads in the last election and probably also in the UK's Brexit referendum. I think that these are all issues that will need to be addressed. They are not political issues. They're not there yet.

I would like to move on just quickly to the to the international part of this. While I agree with Joe on the need for conventions, there is only one convention that works at this point and that is the Budapest convention on cyber crime, recently with the Council of Europe, which is then acceded to by liberal democracies, the U.S., Canada, Mexico, Japan and Australia. They decided to call to Budapest convention because it was no longer a Council of Europe thing.

The problem with that convention, but which may also lead the way to future thinking, is there are a whole host of countries that have not acceded to the Budapest convention, most prominently China, Russia and Belarus. I think Ukraine is somewhere in between because Ukraine, at least up till the end of Yanukovych's regime, was also a primary source of all kind of cyber crime. But rather I direct attention to a fundamental conundrum of cyber security at the international level that we need to address, which is our thinking about security since the first rock by a hominid pre-human hominum was thrown to kill another pre-human hominid, has been kinetic, distance based. Force equals mass times acceleration, meters per second squared. Meters no longer matter in security these days; distance does not matter. All of our security thinking up to the present has been based on the concept of distance, therefore geography. Think about what is the primary security organization that we have, I mean are in it, the North Atlantic Treaty

Organization. Countries that share all of the values of the countries of the North Atlantic Treaty Organization such as New Zealand Australia Japan and Uruguay... they are not in the North Atlantic Treaty Organization simply because they're not in the North Atlantic. All the work of the North Atlantic Treaty Organization is based on things such as tank logistics, fighter range, bomber range, troop movement logistics. It is all distance-space. Today, all of the threats have nothing to do with distance: borders are breached without being noticed. On top of that, the threats, I will take just one, APT28, or Fancy Bear, have hacked the Bundestag, hacked the Italian foreign ministry. They have done all kinds of things to the Netherlands, Sweden, Ukraine. Even the World Anti-Doping Agency has been hacked by this one group of probably GRU hackers. It of course did hack the DNC. I should point out here that David Langer at least told me that of the 126 people working at the DNC with access to the DNC server, 124 were actually using two factor authentication, two were not. Guess how the DNC server got hacked!

Anyway the point is that our ways of looking at things in this side in the digital era just have to change. We have to think about security not in terms of geography. We have to realize that the threats can hit all over and perhaps what is at risk are our forms of government, ways of organizing society. Certainly that is the case what we've seen in the last year or so, not only with attempts to derail the US elections but, we know better that, with the Brexit campaign. We know that, in France, Emmanuel Macron's server was hacked. Having learned from the DNC **hack, t**hey actually loaded their email server with obvious fakes so that when they were docs, published things that were so obviously fake that it disqualified virtually everything, even what was perhaps potentially embarrassing. Nonetheless I would say that we should learn from these individual actions and think about how we should guarantee our security in the future, think about working together a lot more.

Our own experience with this was not very good. From now on every history, cyber warfare begins with the April-May 2007 attacks on Estonia. They were DoT attacks, which meant our systems were never breached, they were just shut off from people. At the time NATO was loath to admit that this had been going on. Slowly people came around and realized that this was a **closet Vicient** event, attenuation of policy by other means. Ultimately what we had been asking for years was a center of excellence in Tallinn which produced Tallinn Manual 1 and 2. It was established in my country but even NATO took a while to get there.

It is sort of the traditional model of you know someone breaches the border and then there is the Article Five. Decision made it **inact** doesn't really hold because in a cyber event, you have problems with the attribution, you don't know what the proper response is. We are just not ready for that or have not been ready for that.

But nonetheless we see the security situation has decreased to such a level that even our democratic systems seem to be under threat. That we have to start thinking in multilateral terms as I mentioned we do have the Budapest convention on cyber crime which kind of maybe gives us an idea of that like-minded nations have agreed that they will work against cyber crime, will give out criminals from their territory. It has been used to great effect in a number of countries where one country identifies a hacker in another country. According to the Budapest convention, they are then extradited.

We see that other areas do not work so well as Joe mentioned. **Ungar has f**ailed this year. That's because during the ITU discussions about five years ago, already then a set of like-minded countries, China, Belarus, Russia were basically arguing for what would amount to censorship of the web because their definition of security is of information security, is not devoted to hacking, to hacking other people's infrastructure. It includes freedom of speech and that's clearly something that liberal democracies are not willing to put up with. Another example of fairly successful cooperation that also might lead the way is the possession of the NATO center in Tallinn because while it was originally open only to NATO countries that it is now open to other like-minded nations. Finland is a non-NATO member**.** Japan basically has asked "we could we join, Is that fine"? It is a long decision making process there but if we are as we have seen with threatening both at the level of infrastructure, at the level of privacy, at the level of of our democratic processes, we will have to develop at least among liberal democracies some kind of defensive mechanisms among them, international cooperation. At this point or until perhaps two weeks ago,

there has been no real cooperation within NATO. NATO's idea of cyber security is only to deal with the security of the organization, not the members or the allies but just the organization.

Thinking is moving beyond that but maybe has not gone far enough. I do think we will have to face up to the reality that liberal democracies are under threat, that the mechanisms for attacking

liberal democracies are no longer merely kinetic and that we have to start working toward some kind of serious organization for cyber security for liberal democracies that as with the attacks transcend geographical boundaries from New Zealand and Australia to Finland and Estonia, countries will share information. It is going to be a long time cyber information even within NATO as I said. It is more a matter of following the espionage paradigm where you do not share anything as opposed to the interoperability paradigm that you put a U.S. missile under a French Mirage jet. It means in that sense interoperability. In fact, it is one of our experiences when we discovered some malware, we went to NATO and said oh look what we found in NATO said Oh you too to an ally. That is not how you do cyber security, frankly. So I would argue in close with that we do need to think about these things.

I will close with two small points. One of them is that we hear everywhere all this talk about we need backdoors. We have seen the Prime Minister of Australia, the Commissioner of Justice for the European Union, the Minister of Home Affairs in the UK, the U.S. attorney general also argue for backdoors. I do not understand that issue, frankly. Why you would want to do that?

Or maybe because it comes from not understanding technology basically soon as you have a backdoor that becomes the Holy Grail, the Holy Grail for the people because it is one stop shopping. Why would you want to try to hack anyone if there is a hackable key, a backdoor somewhere and we need not think only in terms of smart people hacking a key. We know CIA and NSA have been hacked but you do not even need that. The worst cases of breaches have been insider threat. Scott Sagan just put out a whole collection of insider threats but think about what is one of the worse case than Snowden? No one breached NSA. He was an insider threat. Reality winner that bizarrely named woman who just gave out an NSA document on Russian attempts to hack voting machines. It is an insider job. Now I take not to criticize the United States, so to say. In the European Union, 500 million people, the commissioner for Justice says OK it gets a wish and the wish is to have a backdoor key. Now if I am Vladimir Putin or someone else, I would say OK I do not have to hack anything, I just need the key I can get into everything. And instead of its that of trying to get in there through digital electronics means, I would just find out who the key master is, say I give you two billion euros, eventually you find someone who is going to fall for that.

So let's stay away from backdoor keys. My point in this regard, I should say, that Estonia which the ITU has listed Estonia as the most secure, in terms of cyber security, country in Europe. Russia is the most secure in Eurasia, China is the most secure in Asia. The only difference is that the Freedom House has also rated Estonia as number one in the world in freedom online, which disputes the argument that you need to be repressive in order to have security in cyberspace.

Ultimately everything boils down to my mind to a brilliant essay (it was not that brilliant but the ideas in it were brilliant). It was written 58 years ago, in 1959, by C.P. Snow called "The Two Cultures" which I think was not nearly as relevant when it was published as it is today. C.P. Snow was a physical chemist and a literary novelist who gave the world the term the corridors of power in one of his novels. But he had this great little essay about being at the faculty dining club in his College in Cambridge sitting with the physical chemists, the physicists, the other chemists discussing presumably quantum mechanics and then he would get up after dinner and go drink with the poets and the essayists and the novelists and the Shakespeare scholars. I mean he was the only one who could move between the two tables. The poets and essayists had no clue about physics and the physicists and the chemists could not care less about literature. And he said this is a problem of the university. I would argue today it is a problem of society. Be back then technology did not impinge upon people's lives the way it does now.

Your phone did not tell anyone where you were, it was plugged into the wall. The most you had to do, your greatest, your television could not look at you so despite the sort of all well-being published already ten years earlier but you did not need to put a little thing in front of your computer to keep the computer from looking at you or listening to you. The most you interact with technology perhaps was to set the timing on your distributor cap which is something the most people under 40 do not even know what it is. So it was a different world today: technology impinges upon us everywhere. Yet people do not understand the problem of this. Technologists do not understand the ethical, legal, moral, philosophical basis of a liberal democracy in many cases and the people who are responsible for the legal system do not have a clue about IT.

On the one hand, right after the iPhone came out, with one of the early apps you could find out where you traveled. I downloaded the app and I got this map of where I had been all based on the

S7 protocol that says the mobile phone has been big fat lines where I traveled a lot and thinner gray ones where I did not. I showed it to security detail and they said eliminate that immediately. I said what is the point? I mean the data exists, so someone else can have it.

And then again 2014, in the Fall, I went to went to the European Parliament. They have a five-year term. It was half a year after their most recent election I gave a talk about digital stuff, trying to tell them how important it is, that you actually know something about it. And as a kind of show and tell moment I pulled out my mobile phone and I said this thing here you all have one everyone had one of course. Thank you so much.