EUROPEAN COMMISSION

[CHECK AGAINST DELIVERY]

Neelie KROES
Vice-President of the European Commission responsible for the Digital Agenda

A secure online network for Europe

Cyber security conference
Brussels, 28 February 2014

To add your comment to this speech, see the social version of the speech here

Digital technologies are changing our world.

Today we are already seeing the difference it makes. From cars to classrooms; from payments to power stations.

And this offers huge opportunities for citizens, the society and the economy.

I often focus on the economic opportunities: and they are significant. The Internet economy generates over one fifth of our growth; 200 million Europeans buy online each year.

But it's more than economic. It is also for true believers. As Pope Francis put it recently: good communication helps us to grow closer, to know one another better, and to grow in unity; in his own words, the Internet is a "gift from God".

I don't know if it's really a gift from God. But his words are definitely a gift to the Digital Agenda for Europe.

And what we have seen is just the beginning. On the horizon stand new opportunities: big data, cloud computing, the Internet of things, high performance and quantum computing: you name it.

Of course: like any new advance, these opportunities can be misused. We have the technological ability to do immense, unprecedented things. Many of those things are positive; some are damaging. And increasing reliance means increasing vulnerability.

The massive scale of online spying shows how technology can be used for ill. Invading privacy, invading fundamental rights, eroding trust in the online world: and in our governments. This is totally unacceptable.

As Estonian President Toomas Ilves put it recently, it is as though we have two cultures: those who care about technology and those who care about liberal democracy. And not only do they not talk to each other, but act as if the other didn't exist.

It's time those two worlds learned how to understand and inter-relate with each other. Then we would not have a situation where, for example, mass observation of citizens is seen by some as "acceptable" merely because it is technically possible. Or, on the other side, where policy makers look at big data and can see only dangers and threats instead of opportunities.

People – including me - sometimes about talk about our "digital rights". But I don't think that's quite right. These are not digital rights, nor online rights: they are fundamental rights, and they apply just as much online as off. Whether it is privacy, or freedom of speech, or consumer protection. New technology can enhance our humanity: it should not override our human rights.

In the "real world", those freedoms enjoy protections, checks and balances. In the very different online world, those safeguards may need to be different. But they must be present, at every level: political, organisational, technical. And based on common principles: like transparency, responsibility, and accountability. We need to put our foot down to provide those protections. On that note, I welcome President Obama's speech last month on reforming the NSA: that went in the right direction.

But we also need to ask ourselves the right questions. Not why the US wanted to bug the phones of so many. But: "how did they manage to succeed"? Why are we so unprepared and unsecured against such threats?

You could ask, "why does so much of our data leave Europe"; or you could ask, "why do our citizens prefer American platforms"? And why are our European equivalents unable to compete? Let's not be naïve. Spying is the second oldest profession in the world, and sometimes even combined with the first.

The revelations of Snowden came as a shock to many. But in a sense they were a blessing in disguise and a wake-up call. And that is just what we need right now. At the very moment where we are making the transition to a data-driven economy and society, these revelations could not have been more timely. We can use these insights to ensure a more secure online world, and a competitive advantage for European industry.

We shouldn't lose ourselves in the Snowden debate when it comes to online privacy and security. That's not all there is to building trust online – it's also about the simple things.

It's about people trusting that their personal data on social networks is protected.

About small businesses understanding what their cloud provider is offering.

About citizens having the option to use secure eIdentification - if they don't want to be impersonated.

About children protected and empowered to avoid online risks.

Without security, there is no privacy; nor true freedom. You have no private life if your house has no walls; you are not free to walk the streets if it is not safe to do so.

Those cyber breaches happen for multiple reasons: they are all too common and all too costly. According to one study, over three quarters of small businesses, and 93% of large ones suffered one. Each one can cost up to €50 million: not to mention the reputational damage.

Some – most recently Chancellor Merkel – have called for Europe to have a secure, European network. How would we do that?

For me, the answer starts with how we see security. By seeing it as pivotal to our business models, central to competitiveness. By providing a digital single market, fertile ground for European innovation. By speeding up how we share knowledge, to strengthen the security of products and services.

And by saying 'No' to data protectionism; 'Yes' to data protection. Because we want to keep the huge boost of big data, and the benefits of this open, innovative, unified global network.

This is why, last year, my colleagues Cathy Ashton, Cecilia Malmström and I came up with an ambitious cybersecurity strategy. A series of integrated building blocks to safeguard a secure, open internet for Europe.

One year on, we are making progress. Europe is delivering on these areas.

The EU has a new programme for research and development, Horizon 2020. It strengthens our investment in cyber security, privacy and trustworthy ICT. We already have strong capacity in areas like business software, smart cards, and cryptography: now we can build on that.

We have also just established what is called the "NIS platform": a public-private platform for network and information security. This platform aims, as a priority, to find technology-neutral best practice to enhance cyber security; to stimulate secure ICT solutions; and to improve risk management. The platform will feed into Commission recommendations on cyber security, across the whole IT value chain. Because, as you all know, the chain is only as strong as its weakest link. I hope many of you will take part actively in that platform: if you are not already.

Plus, we are implementing our Cloud Computing strategy — to make this technology and its services more trustworthy and transparent. For example, just this week, ENISA published a verified list of which cloud computing security certification schemes are out there, helping you know which you can trust. And the European Cloud Partnership is finalising its recommendations for next steps, too.

Remember this is our comparative advantage – or could be. One estimate put the cost of the Snowden revelations to US cloud providers at around ten billion dollars a year. And security remains an area of European strength.

Plus, remember there is a global angle. And we have incorporated that view too into our work. As the internet is an open, global network, available for all to participate — so it needs to be governed: transparent, multi-stakeholder, and with global balance. That is the philosophy of our Internet Governance strategy just published.

Just this week the EU achieved its latest milestone: agreement with the Council and Parliament on new laws about electronic identification, authentication and signatures. This will boost user convenience, trust and confidence. And that is exactly what we need!

But: all these building blocks, however excellent, will have no future without resilient and secure networks and systems. That is why we have proposed a Directive on Network and Information Security. It is ambitious and important. It will mean better coordination and risk management – just what we need.

But this is the point where I raise my concern - and ask you for your help.

I know that there are still many and important issues to be resolved around this Directive. And I am very open to good ideas and a detailed dialogue to make it work. Let me make myself clear: we aim for smart and effective cooperation between all Member States and all relevant stakeholders. Today that kind of cooperation is already standard for, say, bio-terrorism: now we need to apply it to tomorrow's digital threats.

We will not reinvent the wheel: but will build on existing and proven structures, and on sound principles.

We will also make explicit what this cooperation means and take into account the experiences and expertise in Member States. When it comes to security – you should rather be an excellent copycat, than a possible underdog.

For risk management, we want our critical infrastructure to have the right security measures in place. Both public and private. Both traditional infrastructure, like energy and transport. And modern, like the internet platforms which all of us, and the digital economy, rely on every day.

Plus, of course, each country needs its own capability: including a Computer Emergency Response Team. I'm proud we've already got our own one in place for the EU Institutions. And we stand ready to play our part, cooperating with all others.

Let me make myself even clearer. If that Directive in the end does not make the necessary improvements, if it would have only a marginal impact on our trusted and secure networks: that will weaken your business, weaken our economy and maybe weaken our society too.

Reliability and trust are key European principles. Not only for society, but for economic competitiveness. A weak link will let down the whole network. A weak Directive will let down Europe.

The next few months will be crucial for this Directive: and I will be working closely with the Parliament and Member States to adopt it by the end of this year.

The Cyber Security Strategy is providing us with the right building blocks, but there is important work still to be done. A strong Directive is a European competitive advantage. A weak one, or none at all, would be a proof that democracy can't manage technology.

I hope you and I all share that same ambition: let's make Europe the world's safest online space!

Thank you.