

Cecilia Malmström

Commissioner responsible for Home Affairs

Stepping up the fight against cyber crime

Check Against Delivery
Seul le texte prononcé fait foi
Es gilt das gesprochene Wort

European Cyber Security Conference – Shared threats, shared solutions

Brussels, 14 June 2011

Ladies and Gentlemen, dear Colleagues,

I'm very happy to be here to discuss how we can develop a more unified European cyber policy. Something that will help us overcome the fragmentation we now face.

Today – and the list of speakers for this conference is a proof – we deal with security in cyberspace from many different points of view.

Internet is a wonderful innovation and makes life easier for us in most ways we can think of. It does not matter if you are in Brussels or in Benghazi, you depend on the Internet.

At the same time we also have to acknowledge the less good things with the Internet. Some parts of the cyberspace resemble dark alleys in not so-safe parts of town where we might face robbery, fraud or other crimes.

Considering recent attempts at international level, most recently at the G8 Deauville summit in May, to agree on norms for behaviour on the Internet, I am tempted to describe the current situation in a simpler way:

Maybe we just realise that the cyberspace simply is not so different from our traditional spaces of social interaction.

Sometimes I hear people saying that we politicians exaggerate the cyber threat and that the problems on the Internet will be sorted out by themselves. These comments make me a bit worried.

There is no doubt that threats in cyberspace are very much real ones. Estonia, a co-organiser of today's event, knows this better than most others and has drawn important conclusions for all of us.

The number of cyber attacks in the world is on the rise and the cost of cybercrime is skyrocketing. You can hardly open a paper these days without reading about some major cyber attack. This weekend we could read about the attack on IMF.

The EU institutions are far from immune. Some time ago it was our Emission Trading System that was hacked into, and more recently the institutions themselves became victims of a large-scale cyber attack, severely affecting our e-mailing systems.

I discovered it myself when I couldn't access my e-mails while being on mission in Cairo. That was quite annoying, as e-mailing has become almost as normal as breathing in our modern society. But what is worse is that the intruders attacking the Commission did not only want to create damage. They were there to get important information.

This incident helped to speed up the creation of the Computer Emergency Response Team (CERT) for the European Institutions. The CERT is now active since beginning of June.

Based on all cyber attacks we have seen recently, I don't think I exaggerate when I say that this must be the golden age for cyber criminals. Our job is to change this – and we will. But it can only be done if we join forces.

Given the fact that an attack can happen in 12 countries in 12 seconds, we have to work together. The criminals already do it. And we see an unfortunate trend that more and more of the committed online crimes are of an organised nature.

So what is the way forward? The EU must become better in ensuring security in cyberspace. This includes preventing and fighting cybercrime, as well strengthening the security of our networks.

Cyber security and cyber crime are two sides of the same coin. There are not – and should not be – any artificial dividing line between the two.

The European Commission takes these issues very seriously. I work closely with Vice President Neelie Kroes and High Representative Cathy Ashton in coordinating a joint response to the challenges we are facing.

Policy-wise, the European Institutions have put important pillars on the ground: cyber-security figures prominently in the External Security Strategy, in the 2010 Digital Agenda and in the first ever Internal Security Strategy adopted late last year. These are all steps towards the same goal.

The Internal Security Strategy lists cybercrime and cyber security as one of our main security challenges for the coming four years.

And let me be clear. Member States and EU institutions, public and private sector are in this together. If we fail, the prize will be very high for all of us.

The strategy focuses on three main areas.

The first area is capacity building in law enforcement and the judiciary. Europol is becoming an increasingly important actor in fighting cybercrime and I welcome its efforts to further look into how the agency can be of even bigger support to Member States.

But the Commission and Europol can only be complementary to Member States. Therefore, I encourage Member States to step up their efforts at the national level. How to tackle cybercrime differs a lot across the EU. The European Commission is ready to facilitate platforms to share best practises.

Another area where I want us to work closer together, and where the potential for cooperation is huge, is training. The European Commission has contributed to the development of cybercrime training courses and centres of excellence in the last 10 years and the demand has never been greater.

Just a couple of days ago we have witnessed two important events: the official launch of the 2Centre project in Dublin and France, and the opening of the Belgian Cybercrime Centre of Excellence for Training, Research and Education. Both initiatives have been supported by the Commission.

One major component in the fight against cybercrime will be the establishment of a European Cybercrime Centre by 2013. This centre will become the focal point in the EU's fight against cybercrime and it will also ensure faster reactions in the event of cyber attacks.

We have launched a feasibility study to see what the centre should focus on and where it could be hosted. This study will be the basis for a discussion with Member States early next year.

The input from Member States, industry, and other security organisations will be very important. In the end, the value of a European Cyber Crime centre follows the classical recipe of "You get out what you put in".

The second area is to enhance cooperation with the industry in order to empower and protect citizens.

Much remains to be done to raise the risk awareness of the everyday visitor in cyberspace. It is astonishing to see how many people are still unprotected on the net – without or with outdated anti-virus protection, no firewalls and using computers with unsecured access points.

The cooperation with industry must therefore include building resilience of network and information infrastructure via public-private partnerships, but also dealing with illegal activities on the Internet.

And let me be clear on this. Without the industry taking a bigger responsibility we will not make it. Therefore, we have a shared responsibility to push this dialogue forward.

The third area is to better deal with cyber attacks. This is probably the biggest threat we face today. A major component will be improved cooperation of Member States' computer emergency response teams (CERTs), which are to be set up by 2012. In this work ENISA, but also Europol, will have important roles to play.

All these actions will make a difference. But we can only be successful if we make the different pieces work together.

The European Cybercrime Centre is a good example. To achieve its goals, the centre has to establish close cooperation with ENISA, as well as with national and governmental CERTs on law enforcement aspects of cyber security.

The interface of this planned Centre and the private sector is of utmost importance. It comes as no surprise that a great number of cybercrimes – including bigger attacks – are never even put on record by law enforcement agencies due to the simple fact that such cases are never reported in the first place. This has to change.

We must encourage citizens and companies to report crimes more often. How can we otherwise solve crimes if they are not reported? Also, without reports on crimes, we cannot understand the operational patterns of the criminal actions.

Improvements in these three areas – law enforcement, cooperation with industry to empower the citizens, and building capabilities to prevent cyber attacks - are crucial, but they will not be enough. Cybercrime is a global problem, so it goes without saying that it needs a global response.

Europe's main partner is the United States. That is why the creation of the high-level EU-US Working Group on cyber security and cybercrime, agreed at the November EU-US summit last year, is so important.

The group should deliver concrete results within one year. This will include everything from preparing joint exercises to fight child pornography, and to develop a public private partnership with the industry.

Besides working with the US, I would also like to mention the contacts established between the EU and NATO. No actor will be able to handle the cyber threat alone. This is why we need to have a dialogue with partners like NATO on how we jointly enhance the security of our citizens.

Ladies and Gentlemen,

Let's take a moment to talk about the rules governing cyberspace. An important but at the same time very complicated issue. This year marks the 10th anniversary of the Council of Europe's Budapest convention on cybercrime. 10 years of cybercrime cooperation in the fast-paced world of today is already an achievement.

Considering that preparatory works on the Convention drafting started in the mid-1990s, it is still an impressive up-to-date instrument. Let us also recall that the EU has said that the Convention should become the legal framework of reference for fighting cybercrime at the global level.

Unfortunately, not all EU Member States have yet ratified the convention. I am happy that the United Kingdom has done so on 25 May 2011, and I understand that Belgium is close to ratifying the Convention as well.

That still leaves 8 countries (Austria, the Czech Republic, Greece, Ireland, Luxembourg, Malta, Poland and Sweden). I know that some of them are preparing for ratification, but I can only urge them to speed up the efforts and will, jointly with the Council of Europe, address a letter to the respective governments.

How influential the Budapest convention is for the EU is well explained in our recent proposal for a Directive on attacks against information systems.

In fact, the text is largely based on the Budapest Convention. What has been added is the part covering large scale attacks, which is an emerging trend not fully covered in the Convention.

The proposal was discussed in the Council last week and the Hungarian Presidency has shown a strong leadership and achieved a general approach. I would like to express my gratitude to the Hungarian efforts and hope that the incoming Polish presidency will keep up the pressure to quickly adapt our legislation to face the challenges of today.

To conclude, let me return to where I started. If we are to take the cyber criminals offline, we need more action from Member States as well as from the EU Institutions and the industry.

We also need to come out of our respective specialist domains, be it industry, law enforcement or security. Information on new threats and possible remedies has to be shared efficiently. Trust has to be built.

What is at stake is nothing less than our citizens' freedom and security on the Internet.

But even though it will be a long and bumpy ride, I'm convinced that we are on the right track to end the golden age for the cyber criminals.

Thank you for your attention.