European Commission - Speech
[Check Against Delivery]

Opening remarks by Vice-President Margaritis Schinas at the press conference on the cybersecurity strategy

Brussels, 16 December 2020

We are back in front of you today with a second security package in as many weeks. This shows our determination to make the Security Union a reality.

We do not need to look far to see why this is also a necessity at the current juncture.

Last September the Dusseldorf University Clinic in Germany was hit by a ransomware attack, which crippled the entire IT network of the hospital and forced Health staff to direct emergency patients elsewhere.

The cyberattack resulted in a woman seeking emergency treatment for a life-threatening condition dying after she had to be taken to another city for treatment. This has been reported as the **first cyber-related death**. Last week, cybercriminals did not hesitate to target the **European Medicines Agency**, with the risk of jeopardising the approval timetable of vaccines against Covid-19. And across the Atlantic, the hacking of the **US Treasury and Commerce departments** shows that even public administration is not immune to cyber threats.

These events clearly show that a cyber incident goes beyond the digital single market or even the digital world.

Cybersecurity is most and foremost about security. Our collective and individual security.

Cybersecurity is ultimately about protecting our European way of life.

Cyber threats are one of the biggest threats to national security, eclipsing even terrorism.

This is why it is so crucial that we are able to provide the basic assurance to Europeans that whenever they connect to the energy grid or get on a plane, or use technology for doing business or as part of their everyday life that **basic security will be provided by a Europe that protects.**

This cybersecurity strategy we are presenting today will pave the way for a better security for all in the EU; it will work as a shield protecting us against the evolving cyber threat landscape. It will support the EU in enhancing its cybersecurity capabilities, preparedness and resilience.

The first deliverable of our new cybersecurity strategy is the **review of the Network and Information Systems Directive and the proposal to update and upgrade the Directive on the protection of our critical infrastructure across the EU, which we are presenting today – immediately turning words into action.**

And the first tangible proof is the proposals on our critical infrastructure which we are finally aligning so that they offer the same level of protection to the most vital parts of our society rendering Europe a pioneer in this respect.

Network information System Directive II

Let me start with the first. The NIS is the first piece of EU-wide legislation on cybersecurity cross-sectorial and in an horizontal way. It helped the EU to develop a culture of cooperation and exchange of information. But although it is a relatively new Directive, its implementation already showed that there is space for improvement.

We need to reach across the EU the same level of cybersecurity and also to promote a security by design.

With the review of the Directive we aim to tackle all the weaknesses we have spotted during the implementation of the NIS I and we also provide to the EU with a modern legal framework which corresponds to the threats and risks we face today and tomorrow.

One of the biggest novelties is the way in which the operators of essential services are identified, which from now on will be based on a size-cap, rather than relying on Member States to identify the operators themselves. **This is an important step towards a more European system, where we can be assured that the same operators all meet a minimum level of standards in a harmonised way, across the EU.**

The reformed NIS Directive will provide the basis for more specific rules that will also be expanded to a larger range of strategically important sectors, including energy, transport and health.

And beyond these reforms, where Europe is taking the lead in NIS is **stepping up enforcement**. In a world where our dependency on the digital systems of critical infrastructure, **we are proposing concrete references for high levels of fines for operators who infringe the requirements of the Directive whether they are essential (e.g. banks, energy or transport operators)** or important (manufacturing industry including computer equipment). **This is where we will also break another silo – the silo of the private sector not cooperating with public authorities on security matters.**

Critical Infrastructure

Unlike the NIS rules, our rules on critical infrastructure are now quite old, dating from 2008 and what we do have today is very narrow in scope, covering only two sectors: energy and transport.

This was a first step of us building our competence in this area but what we've seen since then is that the existing framework is no longer fit for purpose.

It doesn't reflect the evolving threat picture of the critical infrastructures being targets, it is out of touch with what Member States are themselves doing and it doesn't take into account the increasing risk of cross-border cascading effects affecting potentially the whole single market.

The time has therefore come to update and reinforce our existing framework.

The two major novelties of this reform are the broad expansion of the sectors covered (the same as the NIS), as well as to look more at resilience and the ability of critical infrastructures to 'bounce back'.

In designing this new proposal, we sought the maximum possible alignment with the rules on network information security, because where one addresses cyber threats and the other physical, the reality is that the two are inextricably linked.

This is also the whole logic of the Security Union strategy, overcoming the **false dichotomy between online and offline, between digital and physical, between internal and external security concerns** and breaking down the silo approach.

With our proposals today we are building some more compact and well cemented chambers/rooms of the single roof Security house we presented last July.

Thank you for your attention.

SPEECH/20/2460

Press contacts:

Johannes BAHRKE (+32 2 295 86 15)
Adalbert JAHNZ (+ 32 2 295 31 56)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email