High common level of network and information security across the Union. NIS Directive

2013/0027(COD) - 05/12/2013

The Council took note of the **state of play** regarding a draft directive aimed at ensuring a high common level of security of electronic communication networks and information systems across the EU.

Although all delegations fully acknowledge the need for action to combat cyber attacks, **views differ on the best way to ensure network security** throughout the EU:

- some delegations prefer a **flexible approach**, with EU-wide binding rules limited to critical infrastructure and basic requirements, complemented by voluntary measures;
- other delegations, as well as the Commission, consider that only **legally binding measures** would bring about the necessary security at EU level.

As regards more **detailed provisions**, further discussion is needed on a number of questions, such as:

NIS strategy and NIS competent body: delegations acknowledge that a substantial disruption in one Member State can also affect other Member States and could support the principle of a coordinating entity at national level. However, in particular those Member States, which already adopted NIS strategies, designated competent bodies and set up a national computer emergency response teams (CERT), seem to critically look at chapter II of the proposal, which deals with the national framework on NIS: they wish to make sure that the requirements that will have to be met by Member States are consistent with and do not go beyond the current national practice.

Other delegations seek further clarification about the terminology used in this chapter, such as 'risks' and 'threats' and wonder what the exact requirements are and also question whether these requirements should only concern the private sector or also the public sector.

Competent authority and its task description: many issues require further clarification, such as whether the authority should assume operational tasks, which is something many Member States object to, and what should be the division of responsibilities with the national CERT.

Risk management and incident notification: many delegations:

- doubt whether in addition to 'operators of critical infrastructures', also 'information society service providers' should be covered by the proposal;
- called for more clarity on the definition and for more flexibility for Member States to define which sectors constitute national critical infrastructures. Some delegations wish to limit the proposed requirements to the private sector only and others call for the security breach reporting requirements in this chapter to be voluntary;
- questioned whether or how Member States could actually "ensure" that parties secure their networks and notify incidents.

There are also concerns with regard to the implications of notifications on matters of privacy and confidentiality of information.

Cooperation network: further discussion will be needed on the tasks of the cooperation network although many delegations are of the opinion that it should not assume any operational tasks; some argue in this respect that it would be better to refer to a mechanism rather than to a network.

A number of organisational issues also require further clarification, such as:

- who will chair the cooperation network, what its costs would be, and what the relationship and division of responsibilities would be with the cooperation of national CERTs with ENISA and with Europol;
- the sharing of information in the network should be done on a voluntary basis;
- the question of the need for the proposed and dedicated 'secure information-sharing system';
- the proposed early warning mechanism raises many queries and concerns, e.g. which information shall be shared at what point in time and with what possible consequences for the incident or risk;
- the question of the scope of the proposed coordinated response mechanism and when and under what conditions a coordinated response would be required requires further discussion.

According to the Presidency, the main challenge will be to agree on an approach, which strikes the **right balance between EU-wide binding rules and optional, voluntary measures**, all of which should lead to similar levels of NIS preparedness among the Member States and allow the EU to respond effectively to NIS challenges.