COUNCIL OF THE EUROPEAN UNION

Brussels, 28 May 2013

10076/13

Interinstitutional File: 2013/0027 (COD)

TELECOM 136
DATAPROTECT 68
CYBER 11
MI 449
CODEC 1209

NOTE

from:	Presidency
to:	Delegations
No. Cion prop.:	6342/13 TELECOM 24 DATAPROTECT 14 CYBER 2 MI 104 CODEC313 + ADD1 +ADD2
No. prev doc. :	9745/13 TELECOM 125 DATAPROTECT 64 CYBER 10 MI 419 CODEC 1130
Subject:	Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - *Progress report & questions for the orientation debate*

The present report has been drawn up under the responsibility of the Irish Presidency. After putting the proposal in the context of the cyber strategy it sets out the work done so far in the Council's preparatory bodies and gives an account on the state of play in the examination of the above mentioned proposal.

1. THE EU CYBER SECURITY STRATEGY

- On 12 February, the Commission submitted its proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (hereinafter: NIS Directive).[1] At the same time, the Commission and the High Representative of the EU for foreign affairs and security policy submitted their joint Communication on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.[2] The cybersecurity strategy represents the EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks. This is to further European values of freedom and democracy and ensure the digital economy can safely grow. Specific actions are aimed at enhancing cyber resilience of information systems, reducing cybercrime and strengthening EU international cyber-security policy and cyber defence.

- The joint cyber security strategy proposes specific EU-level actions around five strategic priorities: becoming cyber resilient, reducing cyber crime, developing resources for cyber security, developing an EU cyber defence policy and promoting EU core values. The implementation of the strategy would require the involvement of different actors, such as the EU institutions, the EU Member States, the European Network and Information Security Agency (ENISA), Europol (including the European Cyber Crime Centre - EC3), the European Defence Agency (EDA) an other stakeholders.

1 Doc. 6342/13.
2 Doc. 6225/13.

- After an initial discussion in the newly established Friends of the Presidency Group on Cyber issues (hereinafter: FoP Cyber) on 3 December 2012[3], the Commission presented its Cyber security Communication to the FoP Cyber on 25 February[4], where the Irish Presidency announced its intention to invite the Council to adopt conclusions at the General Affairs Council (GAC) of 25 June. In April, the Presidency put together draft Council conclusions on the cyber security strategy, which were based on contributions from all the Council Working Parties concerned with the subject as well as from individual Member States. In line with the mandate of the FoP Cyber the Presidency also clarified that the proposed NIS Directive would be dealt with solely by the WP TELE (see below). On 15 May, the FoP Cyber discussed the draft Council conclusions put together by the Presidency, which, amongst a great number of other things, refers to *achieving cyber resilience* in terms of: securing cyber security and incident response at EU and Member State levels, public-private partnerships, awareness raising on 'digital hygiene', cyber security exercises and EU cooperation and coordination.

2. THE PROPOSED DIRECTIVE ON NETWORK AND INFORMATION SECURITY

- The proposed NIS Directive is based on article 114 TFEU. This proposal is a key component of the overall strategy and would require all Member States, key internet enablers and critical infrastructure operators such as e-commerce platforms and social networks and operators in energy, transport, banking and healthcare services to ensure a secure and trustworthy digital environment throughout the EU. The proposed Directive lays down measures including:

  – Member State must adopt a NIS strategy and designate a national NIS competent authority with adequate financial and human resources to prevent, handle and respond to NIS risks and incidents;

[3] Doc. 17414/12.
[4] Doc. 7062/12.

- Creating a cooperation mechanism among Member States and the Commission to share early warnings on risks and incidents through a secure infrastructure, cooperate and organise regular peer reviews;
- Operators of critical infrastructures in some sectors (financial services, transport, energy, health), enablers of information society services (notably: app stores, e-commerce platforms, Internet payment, cloud computing, search engines, social networks) and public administrations must adopt risk management practices and report major security incidents on their core services.

- The Commission presented the cyber security strategy and its proposal for a NIS Directive and the accompanying Impact Assessment[5] to the Working Party on Telecommunications and Information Society (hereinafter: WP TELE) on 28 February. On 11 April, a first exchange of views on the proposed NIS Directive took place. On this occasion, delegations underlined that they were only able to express preliminary points of view as national consultations on the proposal were still underway. Further to this first exchange of views, several delegations submitted preliminary written comments, either on specific articles in the proposal or more generally on the Impact Assessment and on the justifications given for provisions in the proposal.

- With the purpose of informing the Ministers' debate at the TTE Council of 6 June and on the basis of the preliminary comments from the delegations during the meetings of the WP TELE on 28 February and 11 April and on the limited number of written comments received, the Presidency has identified the following main issues, which it believes are matters delegations would like to discuss further.

[5] Doc. 6342/13.

- With regard to the Impact Assessment (hereinafter: IA), which accompanies the proposal, a number of Member States pointed out that there appears to be a number of discrepancies between the two documents and that in particular the IA does not sufficiently justify why specific sectors have been included in the proposal, such as enablers of information society services, and others not, such as hardware/software manufacturers. Member States were also looking for more substance in the IA with regard to the impact of the perceived proposal on employment, competitiveness and innovation, data protection, operations of multinational companies, investment climate, etc. Most Member States also raised the issue of the perceived significant costs involved in the implementation of the Directive and regretted that the IA fails to sufficiently assess the possible benefits. At a more fundamental level, Member States requested further justification from the Commission why a legislative, rather than a voluntary approach, would be the preferred option to tackle the uneven level of security capabilities across the EU and the insufficient sharing of information on incidents, risks and threats, which the Commission perceives as being the root causes of the situation. Finally, delegations asked for more information about which companies and other stakeholders had replied to which questions in the Commission's public consultation, as this would help them to better assess where urgent problems exist.

- With regard to the scope of the proposal and in addition to what has been mentioned above, detailed discussions will be necessary on which "market operators" would fall within the scope of the Directive. In this regard, doubts were expressed about putting providers of information society services under the same obligations as operators of critical infrastructures and questions were raised with the proposed non exhaustive list of market operators, which would need to be agreed upon and which would cover those entities to which obligations with regard to incidents' notifications would apply. Some Member States suggested including the EU institutions and agencies in the scope of the Directive as all Member States rely on and are connected to EU information systems. More generally, many delegations are unclear how the proposal for a NIS Directive would relate to other relevant pending and forthcoming legislation, such as that concerning critical infrastructures, attacks against information systems, data protection and electronic identification. In particular with regard to the notification of security incidents, Member States are unclear whether the level of safety requirements for public authorities and market operators according to the proposed NIS Directive should be equal to the Framework Directive[6] requirements for providers of electronic communications networks and services --who are excluded from the scope of the proposed NIS Directive. They are also concerned that various notification obligations in several pieces of legislation might lead to confusion.

- With regard to the organisational framework for the implementation of the Directive, which would require national NIS strategies and national and EU cooperation plans and networks and which would involve national competent NIS authorities and Computer Emergency Response Teams (CERTs), delegations have not yet expressed firm positions on the proposed governance structure as they are currently carrying out national consultations with stakeholders and are analysing the details of the proposal in the context of existing or planned national cyber strategies.

[6] Directive 2002/21/EC as amended by Directive 2009/140/EC.

3. QUESTION FOR DEBATE AT THE 6 JUNE TTE COUNCIL

- According to the Commission's impact assessment accompanying the proposal for a NIS Directive, the current situation in the EU, reflecting a voluntary approach followed so far, has not provided sufficient protection against NIS incidents and risks across the EU and has resulted in an uneven level of preparedness in the EU Member States, despite the work carried out in the European Forum for Member States (EFMS), ENISA and the European Public-Private Partnership for Resilience (EP_3R).

The proposal for a NIS Directive comprises legislative provisions regarding information-sharing on cyber-threats between intelligence and law enforcement agencies and private companies that provide or support critical infrastructure, such as operators of energy, transport, banking and healthcare services and internet companies such as payment services, social networks, search engines, cloud services, apps providers, e-commerce platforms, video sharing platforms and voice-over-internet providers. Such companies will be obliged to be audited for preparedness and to notify national authorities of cyber incidents with a "significant impact".

Do you agree that, in order to achieve a sufficient level of protection across the EU against NIS incidents and to provide Member States with a comparable level of capabilities to counter threats and incidents, including of a cross-border nature, the setting of high quality standards in network and information security is best achieved through EU legislation? Or would you rather favour a voluntary or mixed voluntary/legislative approach?

- Considering that other parts of the world, such as the USA, appear to opt for a more voluntary and flexible approach with regard to cyber-security standards, this might create inconsistencies for companies whose operations span several jurisdictions, as is usually the case with many online services.

  Do you believe that EU companies and companies from third countries active in the EU should implement higher security standards than companies in and from other parts in the world? Is there a need to coordinate this matter further at a global level before regional solutions are implemented?

*

* *

Following its consideration by Coreper on 28 May, the Presidency presents this progress report to the Council to take note of it and hold an orientation debate on the questions set out in point 3.