COUNCIL OF THE EUROPEAN UNION

Brussels, 8 May 2014 (OR. en)

9269/14

ENFOPOL 120 TELECOM 109 CYBER 22

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Directive on Network and Information Security

Delegations will find enclosed a letter from the Chairman of the European Cybercrime Task Force (EUCTF) on the draft Directive on Network and Information Security (doc. 6342/13), addressed to the Chair of the LEWP. The same letter was addressed to the Chair of the Telecommunications Working Group, Mr Datsikas.

EUCTF
European Union
Cybercrime Taskforce

The Hague, 24 April 2014

Attn: Chair of the Law enforcement Working Party

Konstantinos Margaros
Hellenic Republic
Ministry of Public Order and Citizen Protection
Hellenic Police HQ
International Police Cooperation Division
1st Section EU, International Relations & Missions

Subject: Directive on Network and Information Security

Dear Mr Margaros,

I am writing on behalf of the European Union Cybercrime Task Force (EUCTF), a forum mandated under JHA council recommendations which comprises of senior representatives (Heads of Cybercrime Units) from law enforcement agencies across all EU Member States. One of the responsibilities of the forum is to advise the EU institutions on relevant cybercrime developments, threats and ways of countering them. I would therefore welcome the opportunity to engage with you on the issue of the Directive on Network and Information Security.

At our recent meeting (8th and 9th April) we held a substantive discussion on the issue of the Directive. I thought it would be helpful to inform the ongoing debate to share the views of EUCTF members.

The EUCTF notes that the Commission has included in its proposal an obligation for a defined set of operators to report "incidents having a significant impact on the security of the core services" to a national authority. This national authority should be entrusted with tasks in the area of network and information security ('NIS competent authority'). In turn, the draft Directive requires the NIS competent authorities to notify law enforcement authorities in case a reported cyber incident is of a 'suspected serious criminal nature' (Article 15.4 of the draft Directive).

The EUCTF considers this a sensible and balanced approach, which ensures that a closely circumscribed set of cyber-attacks with potentially serious impact on the concerned operators but also on society at large might not go unnoticed by national law enforcement authorities.

At present, in most Member States the decision to report cyber incidents to NIS authorities as well as to the police is left to the discretion of market operators. There is clear evidence that businesses severely under-report cybercrime committed against them. This applies not only to reporting to law enforcement but also to reporting to NIS competent authorities.

The limits of this voluntary approach are increasingly being recognised. In this light, a mandatory reporting of cyber incidents should logically include a procedure defining how this information would then be transmitted by NIS authorities to law

enforcement, should the incident be of a criminal nature. Such a mechanism already exists in some Member States, where the cooperation between NIS authorities and law enforcement authorities has already been institutionalised, for example through the definition of working arrangements. It is also important that the transmission of information between the various competent authorities occurs as efficiently and quickly as possible, to ensure that the data needed to support law enforcement investigations- which are by nature very volatile- can be preserved.

The involvement of law enforcement authorities is essential in this area as indeed a significant number of major cyber incidents affecting companies operating essential services (such as electricity and gas suppliers or hospitals etc., which are covered by the scope of the draft NIS Directive) are caused by criminal activity.

Cooperation between all actors, including law enforcement, is of central importance for a number of reasons:

- First of all, failing to give law enforcement a clear role would create a strong imbalance between NIS authorities - whose tasks are limited to prevention, detection and mitigation of incidents - law enforcement authorities can play an equally vital role in the prevention of cyber incidents and also contribute to tackle one of the main causes of the problem, i.e. the growing number of criminally motivated attacks. We consider that the approach currently taken by the draft Directive is the right one to foster a stronger and more collaborative response to cyber incidents, both across borders and across communities, while limiting itself to a closely confined set of serious incidents.

- Furthermore, in today's societies, where core services are highly dependent on IT infrastructures, criminal attacks would very likely have an impact on individuals' safety and on the security of their personal data. The primary victims of cyber-attacks (companies) are not necessarily the ones bearing the most adverse effects of the attack. In many cases, cyber-attacks will also include the theft of customer data or will otherwise affect a number of victims beyond the company targeted. We believe that it should not be left to the discretion of the NIS authority or the company to decide whether or not other victims will be protected.

- This approach is also necessary to provide clarity and legal certainty to operators about the criteria and procedures according to which their data will be shared by NIS authorities once they receive their reports. Carefully defining such criteria and circumstances is therefore important to preserve operators' trust and to ensure the smooth functioning of the internal market. We would suggest the co-legislators may wish to consider putting in place standard procedures and safeguards to ensure the appropriate handling of information also beyond the network of competent authorities.

- Companies are sometimes reported to fear a loss of reputation when information is shared with authorities. It is unlikely in any event that, given their seriousness, the type of incidents covered by the Directive will go entirely unnoticed by the public. The reputation damage – if any – therefore would not be linked to the involvement of law enforcement. In any event, the police are subject to strict confidentiality rules already in most Member States.

The reporting obligation as it is currently proposed would strike the right balance between two objectives: it would enable a more effective response to cybercrime while preserving the positive effects of keeping the reporting of cyber incidents by individuals, SMEs, and non-core sectors businesses entirely voluntary and the reporting of cyber incidents by core businesses also largely voluntary (except for major ones with a clear criminal dimension). It would also contribute to strengthen the cooperation between Law enforcement and judicial authorities on the one hand and NIS authorities and CERTs on the other hand, thereby leading to a clearer and more harmonised approach to information sharing.

We are clear that the current drafting of the provisions on the reporting of cyber incidents in the NIS Directive would have a beneficial impact on the functioning of the internal market and foster cooperation between all involved actors to ensure a higher level of network security. We are hopeful that these negotiations will consider the views of EUCTF ultimately all our intentions are to enable improved protection to EU citizens' safety and their fundamental rights, including the protection of their personal data and privacy.

Yours Sincerely

Lee Miles
Chairman EUCTF.