СЪВЕТ НА ЕВРОПЕЙСКИЯ СЪЮЗ

Брюксел, 22 май 2014 г.
(OR. en)

10097/14

LIMITE

TELECOM 118
DATAPROTECT 77
CYBER 31
MI 446
CSC 111
CODEC 1338

Междуинституционално досие: 2013/0027 (COD)

БЕЛЕЖКА

От:	Председателството
До:	Делегациите
№ предл. Ком.:	6342/13 TELECOM 24 DATAPROTECT 14 CYBER 2 MI 104 CODEC 313 + ADD1 +ADD2
№ предх. док.:	9757/14 TELECOM 111 DATAPROTECT 69 CYBER 27 MI 419 CSC 103 CODEC 1264
Относно:	Предложение за директива на Европейския парламент и на Съвета относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза — Доклад за напредъка

Настоящият доклад е изготвен под ръководството на гръцкото председателство. В него се прави преглед на извършената до момента работа в подготвителните органи на Съвета, отчита се постигнатият напредък в разглеждането на посоченото по-горе предложение и се определят насоки и подходи с оглед на своевременна подготовка на изменен текст на предложението и на преговорите с Европейския парламент.

ПРОЦЕДУРНИ АСПЕКТИ

1. На 12 февруари 2013 г. Комисията представи предложението си за директива на Европейския парламент и на Съвета относно *мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза* (по-нататък директива за МИС) с правно основание член 114 от ДФЕС[1]. Предложението е част от „Стратегията на Европейския съюз за киберсигурност — Отворено, безопасно и сигурно киберпространство[2], относно която Съветът прие заключения на 25 юни 2013 г[3]. На 6 юни[4] и 5 декември[5] Съветът по транспорт, телекомуникации и енергетика взе под внимание осъществения напредък в разглеждането на предложението за Директива за МИС.

2. Европейският икономически и социален комитет[6] и Комитетът на регионите[7] приеха становища по предложението съответно на 22 май и 3—4 юли 2013 г. На 13 март 2014 г. Европейският парламент прие на първо четене законодателна резолюция и 138 изменения, които бяха изготвени от Комисията по вътрешния пазар и защитата на потребителите (IMCO), която е водеща комисия, заедно с Комисията по промишленост, изследвания и енергетика (ITRE) и Комисията по граждански свободи, правосъдие и вътрешни работи (LIBE) в качеството им на „асоциирани комисии“[8].

---

1 Док. 6342/13.
2 Док. 6225/13.
3 Док. 11357/13.
4 Док. 10076/13 и док. 10457/13.
5 Док. 16630/13 и док. 17341/13.
6 TEN/513.
7 2013/C 280/05.
8 Док. 7451/14.

3. По време на гръцкото председателство работна група „Телекомуникации и информационно общество“ (WP TELE) продължи с разглеждането на предложението член по член в рамките на 6 заседания[9]. Като взе предвид обсъжданията в работна група „Телекомуникации и информационно общество“ въз основа на изготвените от председателството документи за обсъждане[10], както и представените в писмен вид бележки от повечето държави членки, гръцкото председателство изготви настоящия доклад за напредъка, който съдържа ключовите въпроси, залегнали в предложението, и, където е възможно, набелязва въпросите, по които държавите членки изразяват принципно съгласие относно начина на действие. Успоредно с доклада за напредъка и с илюстративна цел председателството изготви първия изменен вариант на текста на предложението[11], който беше представен на WP TELE на 26 май и който би могъл да послужи за основа на по-нататъшната работа по време на италианското председателство с цел своевременното започване на преговорите с ЕП.

4. Бяха изразени опасения дали предложеното правно основание (член 114 от ДФЕС) е достатъчно за цялото предложение с оглед на целта, обхвата и съдържанието му. Този въпрос трябва да се обмисли и обсъди допълнително. Правната служба на Съвета ще даде писмено становище.

ВЪПРОСИ ПО СЪЩЕСТВО

Глава I: общи разпоредби (членове 1—3):

5. В общи линии делегациите подкрепят предмета и приложното поле на член 1 („Предмет и приложно поле“) и споделят мнението, че предложената директива следва да бъде съществена част от цялостната стратегия на ЕС за киберсигурност. Председателството смята, че мнозинството от държавите членки биха могли да подкрепят известно прецизиране на член 1 в следния смисъл:

   - *В параграф 1 думата „гарантиране“ следва да се замени с „постигане“ или „улесняване“, за да се отрази фактът, че държавите членки не могат, нито поотделно, нито колективно, изцяло да „гарантират“ устойчиво равнище на МИС.*

---

9 На 27.2., 13 и 28.3., 10 и 28.4 и 21.5.2014 г.
10 Док. 7404/14.
11 Док. 10061/14.

- *Вместо да се създава нов „механизъм за сътрудничество“ между държавите членки, параграф 2, буква б) следва да използва съществуващите договорености за „обединяване“ на държавите членки с цел прилагане на директивата на стратегическо/политическо равнище. Би могъл да се проучи въпросът за по-конкретно оперативно сътрудничество, евентуално на доброволна основа, например в рамките на CERT*[12] *и/или компетентните органи.*
- *Засегнатата от инцидент държава членка и/или нейният CERT следва да реши дали и до каква степен съответната информация (и евентуално личните данни) следва да бъде споделена, като отчита интересите в областта на националната сигурност и съответното законодателство, по-специално във връзка със защитата на личните данни или атаките срещу информационните системи.*
- *Във връзка с необходимостта от правна яснота, както е посочено в точка 4 по-горе, допълнителен въпрос, на който трябва да бъде намерено решение, е дали и до каква степен „публичните администрации“ следва да бъдат включени или изключени от обхвата на предложението (в частност член 14).*

6. В общи линии делегациите подкрепят член 2 („Минимална хармонизация“).
7. Във връзка с определенията в член 3, като отбелязва необходимостта от преразглеждането им с напредването на работата, председателството смята, че делегациите като цяло подкрепят следните принципи:
   - *В списъка на определенията следва да се въведе ново определение за „основни услуги“, което да даде възможност по-точно да се определи кои са доставчиците на тези „основни“ услуги, както и да се оцени рискът или „заплахата“ за сигурността и непрекъснатостта на тези услуги.*
   - *Директивата следва да се позовава на списък на общи сектори с критична инфраструктура и да предвижда критерии за определяне на участниците в тези инфраструктури.*
   - *Необходимо е вижданията на държавите членки да се конкретизират по отношение на степента на детайлизиране на текста на директивата, (по-специално на ПРИЛОЖЕНИЕ II), например дали и до каква степен директивата следва да обхваща и „услугите на информационното общество“ и „субектите с ключова роля за предоставянето на интернет услуги“.*
   - *Необходимостта от включването на допълнителни определения следва да се разгледа по-нататък, например относно критичните услуги, свързани с информационните технологии, националния план за управление на риска, стратегията за МИС и плана за сътрудничество.*

[12] CERT означава екип за незабавно реагиране при компютърни инциденти. Беше повдигнат въпросът дали няма да е необходимо в директивата да се използва различна терминология, предвид факта че CERT е регистрирана търговска марка на ЕС, например екип за реагиране при инциденти с компютърната сигурност (CSIRT).

Глава II: национални рамки за МИС (членове 4—7)

8. Като цяло делегациите подкрепят заличаването на член 4 („Принцип“).

9. По отношение на член 5 („Национална стратегия за МИС“) председателството установи, че е налице широка подкрепа по следния въпрос:

   - *Въпреки че по принцип се подкрепя разработването на стратегия за МИС, включително план за сътрудничество, текстът на този член следва да се съсредоточи в по-голяма степен върху „жизнеспособни“ общи принципи, отколкото върху конкретни изисквания към стратегията за МИС и плана за сътрудничество, защото подобен подход би бил по-полезен за изграждането на доверие.*

10. По отношение на член 6 („Компетентен орган“) и като се има предвид принципът на субсидиарност, делегациите като че ли подкрепят подход, който би бил надлежно съобразен със съществуващата практика в държавите членки:

    - *Директивата следва да позволи на държавите членки достатъчна гъвкавост при определяне или запазване на един или няколко секторни и ориентирани към политиката компетентни органи.*
    - *Въпреки това всяка държава членка следва да посочи „единно звено за контакт“, чиито задачи трябва да бъдат определени допълнително.*

11. Що се отнася до член 7 („Екипи за незабавно реагиране при компютърни инциденти (CERT)“), държавите членки по принцип подкрепят изискването на директивата да се създадат един или няколко екипа CERT, които могат да бъдат сформирани в рамките на „компетентния орган“ или „единното звено за контакт“ и са съгласни с предложените насоки относно CERT, съдържащи се в док. 7404/14, и по-специално:

    - *Държавите членки следва да запазят достатъчна гъвкавост по отношение на техническата организация и финансовите и човешките ресурси на CERT, което следва да бъде отразено в текста на този член и на ПРИЛОЖЕНИЕ I, но въпреки това директивата следва да бъде категорична по отношение на степента на амбициозност на целите, които трябва да бъдат постигнати, и изискванията за CERT и сътрудничеството между тях.*

Глава III: сътрудничество (членове 8—13)

12. Глава III от предложението обхваща архитектурата на сътрудничеството за МИС. Според председателството всички държави членки отчитат факта, че чрез известно сътрудничество в целия ЕС биха могли да бъдат постигнати сходни и повишени нива на подготвеност на държавите членки по отношение на МИС, което би могло евентуално и да спомогне за улесняването на общия и съгласуван отговор на предизвикателствата, свързани с МИС, ако и когато е необходимо. Въпреки това са необходими по-конкретни виждания по въпроса как следва да изглежда тази мрежа за стратегическо/политическо сътрудничество и каква би била нейната връзка, ако има такава, със съгласуваното оперативно реагиране при национални и евентуално трансгранични киберинциденти.

13. По отношение на член 8 („Мрежа за сътрудничество“) председателството смята, че делегациите като цяло подкрепят следния подход:

- *Директивата следва да определи политически/стратегически подход по отношение на мрежата за сътрудничество (или „група“), която, от една страна, използва капацитета, който трябва да се създаде съгласно глава II по-горе, и същевременно, от друга страна, по целесъобразност предоставя насоки за определяне на подробни условия за оперативно сътрудничество на съответните инстанции.*

- *Акцентът на реакцията в спешни случаи е отговорност на националните органи, например CERT и/или компетентните органи и, при необходимост при случаи (с трансграничен характер) следва да се уточни допълнително, в рамките на установилата оперативно сътрудничество общност от 28-те национални CERT би могло да се установи допълнително сътрудничество на доброволна основа, като евентуално се улесни съгласуван отговор на равнище ЕС.*

- *В рамките на мрежата за сътрудничество следва да се провеждат на доброволна основа партньорски прегледи на способностите и степента на подготвеност.*

14. Що се отнася до член 9 („Сигурна система за обмен на информация“), председателството отбеляза незначителна подкрепа от държавите членки за определянето на задължителни изисквания в директивата относно обмен на (чувствителна или поверителна търговска) информация в мрежата за сътрудничество, за създаването или функционирането на специална сигурна инфраструктура и във връзка с предложената роля на Комисията в този контекст. Като отчита споменатото по-горе, председателството смята, че този член следва да бъде преформулиран в следния смисъл:

- *Директивата не следва да съдържа каквито и да било задължителни изисквания за обмен на информация, което следва да бъде отразено в текста на член 9, или, като алтернативен вариант, този член би могъл да бъде заличен, като се има предвид, че нечувствителна и некласифицирана информация може да се обменя в рамките на мрежата за сътрудничество или съответната информация може да се обменя от CERT и/или компетентните органи.*

15. Що се отнася до член 10 („Ранни предупреждения“), делегациите като цяло изглежда могат да подкрепят общите насоки, определени в док. 7404/14, и по-специално:

- *Предвижданото на ранни предупреждения следва да остане доброволно и обменът на съответната информация в мрежата за сътрудничество следва преди всичко да съдейства за стимулиране на изграждането на доверие между частния сектор и националните компетентни органи, както и между националните компетентни органи.*

- *Що се отнася до атаките срещу информационни системи, тъй като обменът на информация за престъпления е обхванат от директива 2013/40, този въпрос не е необходимо да се разглежда в настоящата директива (т.е. заличаване на параграф 4).*

- *Държавите членки следва да решават дали и каква информация да предоставят в мрежата за сътрудничество (т.е. заличаване на параграф 5).*

- *Ранните предупреждения не следва да възпрепятстват или да забавят националните действия за третиране на заплахите и инцидентите.*

16. По отношение на член 11 („Координиран отговор“) председателството също отбеляза широка подкрепа за насоките, определени в док. 7404/14, и по-специално:

- *Вместо да се създава де факто европейска компетентност за координиране на отговора на ЕС при (национални) инциденти, трябва да се проведе допълнително обсъждане с цел да се изясни дали, кога и в кои случаи следва да е необходим „координиран отговор на ЕС“— дали в случай на големи трансгранични кризи в киберпространството или и в случаите на по-ограничени „ежедневни“ инциденти?*

- *Като се има предвид националната компетентност по отношение на свързаните със сигурността въпроси, директивата по-скоро следва да използва съществуващите разпоредби, за да постигне координация на политиката на равнище ЕС в случай на широкомащабни кризи в киберпространството, отколкото да създава нови и потенциално бавно действащи механизми.*

- *В допълнение към координацията на политиката на равнище ЕС директивата следва да улесни техническото/практическото сътрудничество (напр. между CERT), където би могло да се разработят допълнителни изисквания за оперативен отговор на кризите в киберпространството.*

17. Председателството отбеляза, че въпреки че окончателната позиция на държавите членки относно член 12 („План на Съюза за сътрудничество за МИС“) ще зависи от решенията, свързани с членове 8—11, повечето делегации биха могли да подкрепят прилагането на следния подход по отношение на текста на предложението:

- *Директивата би могла да определи по-скоро „рамка“ отколкото „план“ на Съюза за сътрудничество за МИС, която да бъде насочена към координацията и развитието на политиката и да използва пълноценно съответния експертен опит на ENISA и която да се преразглежда редовно от предвидената в член 8 мрежа за сътрудничество.*

- *„Рамката“ за сътрудничество следва да обхване въпроси като реда и условията за комуникация между CERT, обмена на най-добри практики, повишаването на осведомеността и ученията и обучението, както и да се възползва от експертен опит на ENISA в тази област.*

18. Що се отнася до член 13 („Международно сътрудничество“), председателството отбеляза, че държавите членки искат в текста да се посочи, че всички участващи в рамката за сътрудничеството членове следва да се съгласят в нея да участват и трети държави или международни организации.

Глава IV: сигурност на мрежите (членове 14—16), глава V: заключителни разпоредби (членове 17—23) и приложения I и II: CERT и участниците на пазара

19. По отношение на член 14 („Изисквания за сигурност и уведомяване за инциденти“) председателството отбеляза, че държавите членки, в които националната практика за доброволно уведомяване е довела до задоволително сътрудничество между заинтересованите страни и публичните органи, биха предпочели директивата да използва този опит. Други държави членки попитаха дали в допълнение към това следва да се въведат изисквания за задължително докладване. Всички държави членки изразиха съгласие относно необходимостта от допълнително пояснява на различните изисквания за уведомяване, съдържащи се в различни законодателни актове на ЕС. С оглед на посоченото по-горе председателството би препоръчало допълнително да се разгледа следният подход:

- *Директивата би могла да определи задължителни изисквания за докладване в случай на инциденти със значително трансгранично въздействие, засягащи няколко държави членки.*
- *В случай на вътрешни инциденти с ограничено въздействие държавите членки следва да запазят гъвкавостта да решават, в съответствие с член 2, дали и по какъв начин да докладват на национално равнище.*
- *Директивата следва да зададе параметрите за определяне на въздействието на (секторни) инциденти, но решението дали конкретен инцидент следва да бъде докладван, въз основа на тези параметри, принадлежи на държавите членки.*
- *Държавите членки следва да запазят гъвкавостта си по отношение на реда и условията за докладване на секторните компетентни органи и/или на националното „единно звено за контакт“.*

20. По отношение на член 15 („Изпълнение и правоприлагане“) и въз основа на вижданията на делегациите председателството предлага следното:

- *Директивата следва да предостави достатъчно възможности за национални решения с цел да се постигне по-активно участие на частния сектор от това, което се предлага понастоящем, напр. по отношение на одити на сигурността, развитие на техническите способности, курсове за обучение и т.н.*
- *Директивата следва да предвиди, където е целесъобразно, наличието на множество секторни компетентни органи, които да поемат и отговорности във връзка с изпълнението и правоприлагането.*

21. По въпроса за „стандартизацията“ съгласно член 16, председателството стигна до заключението, че преработването на този член трябва да се обмисли допълнително.

22. Относно член 17 („Санкции“) и по-специално параграф 2 е необходимо допълнително разглеждане с цел да се поясни връзката между директивата за МИС и предстоящия регламент за защита на данните.

23. Накрая председателството отбеляза желанието на делегациите отново да разгледат на по-късен етап „Транспониране“и „Влизане в сила“ (членове 21 и 22) и необходимостта по-късно отново да обсъдят финализирането на ПРИЛОЖЕНИЕ I относно изискванията и задачите на екипите за незабавно реагиране и на ПРИЛОЖЕНИЕ II относно секторите и образуванията, които да бъдат включени в „изчерпателен“ или „индикативен“ списък, в зависимост от преговорите по съдържанието на членовете от предложението.

ЗАКЛЮЧЕНИЕ

24. Гръцкото председателство отбеляза, че всички държави членки без изключение осъзнават неотложната необходимост да се подобри мрежовата и информационната сигурност и да се предприемат действия в тази област на равнище ЕС. Във връзка с това държавите членки отделиха възможно най-голямо внимание на разглеждането на предложението на Комисията и през последните месеци беше постигнат значителен напредък при определянето на посоката, в която следва да се доразвие предложението, както беше обяснено по-горе.

25. Що се отнася до разпоредбите в глави I, II и IV и въз основа на обсъжданията в подготвителните органи на Съвета, председателството смята, че предложените насоки и подходи в настоящия доклад за напредъка следва да бъдат достатъчна основа за доразработването на предложението през периода на предстоящото италианско председателство. Тези насоки и подходи бяха обобщени предвид необходимостта да се намери правилният баланс между подобряването на киберсигурността, изграждането на необходимото доверие и, с цел по-голяма ефективност, пълноценното използване на съществуващия опит, както и избягването на дублирането на експертния опит на съществуващите органи и механизми.

26. Що се отнася до глава III, както беше споменато по-горе (параграф 12), държавите членки изразиха съгласието си по повод необходимостта от укрепване на стратегическото/политическото сътрудничество за МИС на равнище ЕС. Редица държави членки смятат, че директивата следва да предвиди по-конкретни критерии и изисквания за оперативно сътрудничество в случай на инциденти, свързани с МИС. Повечето държави членки обаче смятат, че стратегическото/политическото сътрудничество е най-важният приоритет за изграждането на необходимото доверие и че същевременно редът и условията за оперативното сътрудничество биха могли да бъдат доразработени в контекста на съществуващите механизми и органи. Съгласно предложеното по-горе (параграфи 12—18) председателството не смята, че стратегическото/политическото сътрудничество и оперативното сътрудничество са взаимно изключващи се възможности; според него приоритетът на директивата следва да бъде стратегическото/политическото сътрудничество и същевременно да се предоставят насоки на съществуващите механизми и органи по отношение на оперативното сътрудничество.

*

* *

След разглеждането на настоящия доклад за напредъка от Корепер на 28 май, председателството ще го представи на Съвета и ще прикани Съвета да го вземе под внимание.