Становище на Европейския икономически и социален комитет относно „Предложение за регламент на Европейския парламент и на Съвета относно Европейската агенция за мрежова и информационна сигурност (ENISA)“

COM(2010) 521 окончателен — 2010/0275 (COD)

(2011/C 107/12)

Докладчик: **г-н MORGAN**

На 19 октомври 2010 Съветът реши, в съответствие с член 114 от Договора за функционирането на Европейския съюз, да се консултира с Европейския икономически и социален комитет относно

„*Предложение за регламент на Европейския парламент и на Съвета относно Европейската агенция за мрежова и информационна сигурност (ENISA)*“

COM(2010) 521 окончателен.

Специализирана секция „Транспорт, енергетика, инфраструктури, информационно общество“, на която беше възложено да подготви работата на Комитета по този въпрос, прие своето становище на 2 февруари 2011 г.

На 469-ата си пленарна сесия, проведена на 16 и 17 февруари 2011 г. (заседание от 17 февруари), Европейският икономически и социален комитет прие настоящото становище със 173 гласа „за“ и 5 гласа „въздържал се“.

1. **Заключения и препоръки**

1.1 ЕИСК осъзнава сегашната степен на зависимост на гражданското общество от услугите, предоставяни чрез интернет. Комитетът е също толкова загрижен за относителното невежество на гражданското общество по отношение на собствената му кибернетична сигурност. ЕИСК е на мнение, че Европейската агенция за мрежова и информационна сигурност (ENISA) е агенцията, отговаряща за подпомагането на държавите-членки и доставчиците на услуги при повишаването на общите им стандарти за сигурност, така че всички потребители на интернет да вземат необходимите мерки за осигуряване на собствената си кибернетична сигурност.

1.2 В тази връзка ЕИСК подкрепя предложението за развитие на ENISA с цел да се допринесе за изграждането на високо ниво на мрежова и информационна сигурност в рамките на Съюза и с оглед повишаване на осведомеността и създаване на култура на мрежова и информационна сигурност сред обществото в полза на гражданите, потребителите, предприятията и организациите от публичния сектор в Съюза, като по този начин се подпомогне гладкото функциониране на вътрешния пазар.

1.3 Мисията на ENISA е жизненоважна за сигурното развитие на мрежовата инфраструктура на правителствата, предприятията, търговските дружества и гражданското общество в ЕС. ЕИСК очаква Европейската комисия да приеме най-високите стандарти за работата на ENISA и да наблюдава резултатите от нея в контекста на развиващите се и новопоявяващите се заплахи за кибернетичната сигурност.

1.4 Кибернетичните стратегии, очертани от НАТО, Европол и Европейската Комисия, зависят от ефективното сътрудничество с държавите-членки, които от своя страна имат богат набор от вътрешни агенции, работещи по проблемите на кибернетичната сигурност. Стратегиите на НАТО и Европол са замислени като проактивни и оперативни. В рамките на стратегията на Европейската Комисия, ENISA определено е важна част в сложния пъзел от агенции и мисии за защитата на критичната информационна инфраструктура (CIIP). Въпреки че в новия регламент не се предвижда оперативна роля за ENISA, ЕИСК все още счита, че ENISA е основната агенция, отговаряща за CIIP в гражданското общество в ЕС.

1.5 Оперативната отговорност за кибернетичната сигурност в държавите-членки принадлежи на държавите-членки, но стандартите за CIIP в 27-те държави-членки очевидно са смесени. Привеждането на по-зле оборудваните държави-членки до приемливо равнище е роля на ENISA. Тя трябва да гарантира сътрудничеството между държавите-членки и да ги подпомага в прилагането на най-добри практики. В контекста на трансграничните заплахи ролята на ENISA следва да включва също предупреждаване и превенция.

1.6 ENISA следва също така да участва в международното сътрудничество със сили извън ЕС. Подобно сътрудничество има силен политически характер и в него участват много направления на ЕС, но ЕИСК счита, че ENISA трябва да намери мястото си на международната сцена.

1.7 Комитетът счита, че ENISA може да изпълнява много ценна роля, като допринася и инициира изследователски проекти в областта на сигурността.

1.8 В рамките на оценката на въздействието към настоящия момент ЕИСК няма да подкрепи понастоящем изпълнението в пълен мащаб на варианти 4 и 5, което би превърнало ENISA в оперативна агенция. Кибернетичната сигурност е толкова огромен проблем, с динамично развиващи се заплахи, че държавите-членки трябва да запазят своята способност да се

борят проактивно със заплахите. Резултатът от изграждането на оперативни агенции на ЕС обикновено е намаляване на равнището на квалификация в държавите-членки. В областта на кибернетичната сигурност е вярно обратното – трябва да се усъвършенства равнището на квалификация в държавите-членки.

1.9 ЕИСК разбира мнението на Комисията, че ENISA следва да има ясно определена и добре контролирана мисия със съответстващи ресурси. Въпреки това ЕИСК изразява загриженост, че ограниченият петгодишен мандат на ENISA може да бъде пречка пред дългосрочни проекти и да застраши развитието на човешкия капитал и знанията в агенцията. Това ще е доста малка агенция, натоварена да се справя с голям и нарастващ проблем. Обхватът и мащабът на мисията на ENISA изисква тя да използва специализирани екипи. Работата ѝ ще включва както краткосрочни задачи, така и дългосрочни проекти. Затова Комитетът би предпочел мандатът на ENISA да бъде динамичен и без краен срок, като се потвърждава в текущ порядък чрез периодични анализи и оценки. Тогава средствата могат да се предоставяни на етапи, както и когато това е оправдано.

2. **Въведение**

2.1 Предмет на настоящото становище е регламентът за понататъшното развитие на ENISA.

2.2 Комисията изложи първото си предложение относно политическия подход към мрежовата и информационна сигурност в съобщение от 2001 г. (COM(2001) 298 окончателен). Г-н Retureau изготви обширно становище ([1]) в отговор на съобщението.

2.3 След това Комисията предложи регламент за създаването на ENISA (COM(2003) 63 окончателен). Становището на ЕИСК ([2]) по този регламент беше изготвено от г-н Lagerholm. Агенцията реално беше създадена с Регламент (ЕО) № 460/2004.

2.4 Тъй като използването на интернет продължи да нараства в геометрична прогресия, загрижеността за информационната сигурност непрекъснато се увеличава. През 2006 г. Комисията публикува съобщение, с което очерта Стратегия за сигурно информационно общество (COM(2006) 251 окончателен). Г-н Pezzini изготви становището на ЕИСК ([3]).

2.5 С увеличаването на загрижеността за информационната сигурност, през 2009 г. Комисията излезе с предложение относно защитата на критичната информационна инфраструктура (COM(2009) 149 окончателен). Г-н McDonogh изготви становището ([4]), което беше прието на пленарната сесия на ЕИСК през декември 2009 г.

([1]) ОВ C 48, 21.2.2002 г., стр. 33.
([2]) ОВ C 220, 16.9.2003 г., стр. 33.
([3]) ОВ C 97, 28.4.2007 г., стр. 21.
([4]) ОВ C 255, 22.9.2010 г, стр. 98.

2.6 Понастоящем се предлага ENISA да се укрепи и усъвършенства с цел да се допринесе за изграждането на високо ниво на мрежова и информационна сигурност в рамките на Съюза и с оглед повишаване на осведомеността и създаване на култура на мрежова и информационна сигурност сред обществото в полза на гражданите, потребителите, предприятията и организациите от публичния сектор в Съюза, като по този начин се подпомогне гладкото функциониране на вътрешния пазар.

2.7 ENISA обаче не е единствената агенция за сигурност, планирана за кибернетичното пространство на ЕС. Отговорът на кибернетичната война и кибернетичния тероризъм е отговорност на военните. НАТО е основната агенция в тази сфера. Според новата стратегическа концепция на организацията, публикувана в Лисабон през ноември 2010 г. (достъпна на адрес http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf), НАТО ще „*доразвива способността си за предотвратяване, разкриване, защита и възстановяване от кибернетични атаки, включително чрез използване на процеса на планиране в НАТО за засилване и координация на националните способности за кибернетична защита, за привеждане на всички органи на НАТО под централизирана кибернетична защита и за по-добро интегриране на дейностите на НАТО за осведоменост, предупреждаване и отговор в кибернетичната област с тези на страните членки*“.

2.8 След кибератаката срещу Естония през 2007 г., на 14 май 2008 г. официално беше създаден Съвместен експертен център за кибернетична защита (CCD COE) с цел засилване на способностите за кибернетична защита на НАТО. Установен в Талин, Естония, центърът е дело на международни усилия, включващи понастоящем Естония, Латвия, Литва, Германия, Унгария, Италия, Словашката република и Испания като поддържащи го страни.

2.9 Електронната престъпност на равнището на ЕС е отговорност на Европол. Следва откъс от документ, изготвен от Европол за Камарата на лордовете (виж на адрес http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68we05.htm):

„*Ясно е, че правоприлагащите агенции трябва да не изостават от технологичното развитие на престъпниците, за да гарантират ефективното предотвратяване или разкриване на извършваните от тях престъпления. Освен това, предвид безграничния характер на високите технологии, капацитетът в целия ЕС трябва да е на еднакво високо ниво, за да не се допусне възникването на „слаби точки“, където високотехнологичната престъпност може да процъфтява безнаказано. Този капацитет далеч не е хомогенен в ЕС. В действителност, налице е ясно асиметрично развитие; някои ДЧ се придвижват напред и реализират значителен напредък в определени области, докато други ДЧ изостават в технологично отношение. Това създава необходимост от наличието на централизирана служба, която да подпомага всички ДЧ да координират съвместни дейности, да насърчава стандартизацията на подходите и стандартите за качество и да идентифицира и обменя най-добри практики; само по този начин може да се гарантира хомогенност на правоприлагащите действия на ЕС в борбата срещу високотехнологичната престъпност.*“

2.10 През 2002 г. в Европол беше създаден Център по високотехнологичната престъпност (HTCC). Това е едно относително малко звено, но се очаква да расте в бъдеще като център на работата на Европол в тази област. HTCC играе съществена роля по отношение на координацията, оперативната подкрепа, стратегическия анализ и обучението. Функцията за обучение е особено важна. Освен това, Европол създаде Европейска платформа по киберпрестъпност (ECCP). Тя е насочена към следните теми:

— Онлайн система за докладване на престъпления в интернет (I-CROS);

— Аналитично работно досие (Cyborg);

— Портал за обмен на опит в областта на интернет криминологията (I-FOREX).

2.11 Стратегията на ЕС по отношение на кибернетична сигурност е изложена в глава „Доверие и сигурност“ на Програмата в областта на цифровите технологии за Европа. Посочените предизвикателства са както следва:

„Досега интернет се доказа като забележително сигурен, издръжлив и стабилен, но информационните мрежи и крайните устройства на потребителите остават уязвими за широка гама от увеличаващи се заплахи: през последните години спамът в електронната поща нарасна до такава степен, че сериозно задръства нейния трафик в интернет — делът на спама в електронната поща се оценява на между 80 % и 98 % от всички предавани чрез нея съобщения — и спамът е разпространител на широка гама от компютърни вируси и зловреден софтуер. Нарастващо бедствие са кражбата на самоличност и онлайн измамите. Атаките са с растяща степен на сложност (чрез използване на „троянски коне“, бот мрежи и др.) и често са мотивирани от финансови цели. Възможно е те да са и с политическа мотивация, както показаха неотдавнашните кибератаки, насочени срещу Естония, Литва и Грузия“.

2.12 Заложените в Програмата действия са:

Основно действие 6: Представяне през 2010 г. на мерки за **засилена политика за мрежова и информационна сигурност на високо равнище**, включващи законодателни инициативи като тази за модернизирана ENISA, както и други мерки, позволяващи по-бързо реагиране в случаи на кибератаки, включително екипи за незабавно реагиране при компютърни инциденти (CERT) в европейските институции;

Основно действие 7: Представяне на мерки, включващи законодателни инициативи през 2010 г. за **борба с кибератаки срещу информационни системи**, а до 2013 г. -съответни правила на европейско и международно ниво относно юрисдикцията в киберпространството.

2.13 В съобщение от ноември 2010 г. (COM(2010) 673 окончателен) Комисията доразви Програмата, очертавайки Стратегия за вътрешна сигурност на ЕС. Стратегията има пет цели, третата от които е повишаване на нивото на сигурност на гражданите и предприятията в киберпространството. Предвидени са три програми за действие, като действията са описани подробно в таблицата по-долу (взета от съобщението, достъпно на адрес http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf.

ЦЕЛИ И ДЕЙСТВИЯ	ОТГОВОРНИК	СРОК
ЦЕЛ 3: Да се повишат равнищата на сигурността за гражданите и предприятията в киберпространството		
Действие 1: Да се изгради капацитет в правоприлагащите органи и съдебната система		
Създаване на център на ЕС за киберпрестъпления	Според проучването на приложимостта на COM от 2011 г.	2013 г.
Развитие на способности за разследване и преследване на киберпрестъпления	ДЧ с CEPOL, Европол и Евроюст	2013 г.
Действие 2: Да се работи с предприятията за овластяване и защита на гражданите		
Създаване на процедури за докладване на киберпрестъпления и предоставяне на насоки за гражданите относно кибернетичната сигурност и киберпрестъпленията	ДЧ, COM, Европол, ENISA и частния сектор	постоянен
Насоки за сътрудничество при действията срещу незаконно онлайн съдържание	COM с ДЧ и частния сектор	2011 г.
Действие 3: Да се подобри способността за справяне с кибератаки		
Създаване на мрежа от екипи за незабавно реагиране при компютърни инциденти във всяка държава-членка и един такъв екип за институциите на ЕС. Редовно разработване на национални планове за действие в непредвидени ситуации и тренировки за реакция и възстановяване на системите.	ДЧ и институциите на ЕС с ENISA	2012 г.
Създаване на Европейска система за информационен обмен и предупреждаване (EISAS)	ДЧ с COM и ENISA	2013 г.

2.14 Кибернетичните стратегии, очертани от НАТО, Европол и Европейската Комисия, зависят от ефективното сътрудничество с държавите-членки, които от своя страна имат богат набор от вътрешни агенции, работещи по проблемите на кибернетичната сигурност. Стратегиите на НАТО и Европол са замислени като проактивни и оперативни. В рамките на стратегията на Европейската Комисия, ENISA определено е важна част от сложния пъзел от агенции и мисии за защитата на критичната информационна инфраструктура (CIIP). Въпреки че в новия регламент не се предвижда оперативна роля за ENISA, ЕИСК все още счита, че ENISA е основната агенция, отговаряща за CIIP в гражданското общество в ЕС.

3. **Предложението за ENISA**

3.1 Проблемът, върху който ще работи ENISA, е свързан с действието на седем фактора:

(1) фрагментация и разнообразие от национални подходи;

(2) ограничена способност на Европа за ранно предупреждаване и реагиране;

(3) липса на надеждни данни и ограничени познания за възникващи проблеми;

(4) липса на осведоменост за рисковете и предизвикателствата в сферата на мрежовата и информационната сигурност (МИС);

(5) международното измерение на проблемите в сферата на МИС;

(6) необходимостта от модели на сътрудничество с цел гарантиране на адекватно изпълнение на политиката;

(7) необходимостта от по-ефективни действия срещу престъпления в кибернетичното пространство.

3.2 В предложението за ENISA са съсредоточени както съществуващите политически насоки, така и новите инициативи, изложени в Програмата на ЕС в областта на цифровите технологии.

3.3 Съществуващите политики, които ще бъдат подкрепяни от ENISA, включват:

(i) Европейски форум за държавите-членки (EFMS), чиято цел е насърчаване на дискусиите и обмена в сферата на добрите политически практики с оглед споделяне на политически цели и приоритети относно сигурността и устойчивостта на инфраструктурата на ИКТ,

(ii) Европейско публично-частно партньорство за устойчивост (EP3R), представляващо гъвкава общоевропейска ръководна рамка за устойчивост на инфраструктурата на ИКТ, което функционира чрез насърчаване на сътрудничеството между публичния и частния сектор за целите на сигурността и устойчивостта,

(iii) Програмата от Стокхолм, приета от Европейския съвет на 11 декември 2009 г., която подкрепя политиките, с които се осигурява мрежова сигурност и се дава възможност за по-бързо реагиране в случай на кибернетични атаки в Съюза.

3.4 Новите тенденции, които ще бъдат подкрепяни от ENISA, включват:

(i) засилване на дейностите на EFMS,

(ii) подпомагане на Европейското публично-частно партньорство за устойчивост (EP3R) чрез обсъждане на иновационни мерки и инструменти за подобряване на сигурността и устойчивостта,

(iii) практическа реализация на изискванията относно сигурността, заложени в регулаторния пакет за електронни комуникации,

(iv) улесняване на ученията за подготовка във връзка с кибернетичната сигурност в целия ЕС,

(v) изграждане на CERT за институциите на ЕС,

(vi) мобилизиране и подпомагане на държавите-членки при попълването, а при необходимост и при създаването на национални/правителствени CERT с цел изграждане на добре функционираща мрежа от CERT, покриваща цяла Европа,

(vii) повишаване на осведомеността за предизвикателствата в сферата на МИС.

3.5 Преди изготвянето в окончателен вид на това предложение бяха разгледани пет политически варианта. Всеки вариант беше свързан с мисия и възможности за ресурсното осигуряване. Избран беше третият вариант. Това включва разширяване на функциите, определени понастоящем за ENISA и добавяне на органите за правоприлагане и защита на неприкосновеността на личния живот като заинтересовани страни.

3.6 Съгласно вариант 3, една модернизирана агенция за МИС би допринесла за:

— Намаляване на фрагментацията на националните подходи (фактор за възникване на проблеми № 1), активизиране на политиката, базирана на данни и познания/ информация, и на вземането на решения (фактор за възникване на проблеми № 3) и повишаване на цялостната осведоменост за и справяне с рискове и предизвикателства в сферата на МИС (фактор за възникване на проблеми № 4), чрез допринасяне за:

  — по-ефективно събиране на съответната информация относно рискове, заплахи и уязвими аспекти от всяка отделна държава-членка;

  — увеличаване на наличната информация относно текущите и бъдещи предизвикателства и рискове в сферата на МИС;

  — осигуряване на по-високо качество на политиката в сферата на МИС в държавите-членки.

— Подобряване на европейската способност за ранно предупреждаване и реагиране (фактор за възникване на проблеми № 2) чрез:

  — подпомагане на Комисията и държавите-членки при организирането на общоевропейски учения, постигайки по този начин икономии от мащаба при реагирането на инциденти, засягащия целия ЕС;

  — улесняване на функционирането на EP3R, което в крайна сметка би могло да доведе до нарастване на инвестициите в резултат на общи политически цели и стандарти за сигурност и устойчивост, приложими в целия ЕС.

— Насърчаване на общия глобален подход към МИС (фактор за възникване на проблеми № 5) чрез:

  — увеличаване на обмена на информация и познания с държави извън ЕС.

— По-ефективна и ефикасна борба с престъпленията в кибернетичното пространство (фактор за възникване на проблеми № 7) чрез:

  — ангажиране със задачи с неоперативен характер, свързани с аспекти на МИС, по отношение на правоприлагането и съдебното сътрудничество, като например двустранен обмен на информация и обучения (например в сътрудничество с Европейския полицейски колеж - CEPOL).

3.7 При вариант 3, ENISA ще разполага с всички необходими ресурси за изпълнение на дейностите си по удовлетворителен, задълбочен начин, т.е. създават се условия за реално въздействие. При наличие на повече ресурси ([5]) ENISA може да поеме много по-проактивна роля и да предприема повече инициативи за стимулиране на активното участие на заинтересованите страни. Още повече, тази нова ситуация ще гарантира повече гъвкавост за бързо реагиране на промените в постоянно еволюиращата среда на МИС.

3.8 Вариант на политика 4 включва оперативни функции при борбата срещу атаки в кибернетичното пространство и реагирането на инциденти в кибернетичното пространство. В допълнение към посочените по-горе дейности, Агенцията ще поеме оперативни функции като играе по-активна роля във връзка с CIIP на ЕС, например при предотвратяване и реагиране на инциденти, по-специално функционирайки като CERT на ЕС във връзка с МИС и чрез координиране на националните екипи за действие при инциденти в информационната сигурност като кризисен център на ЕС по отношение на МИС, като това включва както ежедневни управленски дейности, така и спешни действия.

3.9 Вариант 4 би оказал по-голямо въздействие на оперативно ниво, в допълнение към въздействията, които да бъдат постигнати съгласно вариант 3. Функционирайки като екип на ЕС за действие при инциденти в информационната сигурност (CERT) във връзка с МИС и чрез координиране на националните екипи за действие при инциденти в информационната сигурност, Агенцията би допринесла например за по-големи икономии от мащаба при реагиране на инциденти, засягащи целия ЕС, както и за по-ниски оперативни рискове за предприятията поради по-високи нива на сигурност и устойчивост. Вариант 4 би изисквал съществено увеличение на бюджета и човешките ресурси на Агенцията, което буди притеснения относно капацитета ѝ за усвояване и ефективното използване на бюджета по отношение на очакваните ползи.

3.10 Вариант на политика 5 включва оперативни функции в подкрепа на правоприлагащите и съдебните органи при борбата срещу престъпленията в кибернетичното пространство. В допълнение към изброените във вариант 4 дейности, този вариант би дал на ENISA възможност:

— да предоставя подкрепа във връзка с процесуалното право (вж. Конвенцията за престъпленията в кибернетичното пространство): например събиране на данни за трафика, прехващане на данни за съдържанието, мониторинг на потоците в случай на атаки от типа „отказ на услуги“;

— да се превърне в център за експертен опит по отношение на разследване на престъпления, които включват аспекти на МИС.

3.11 Вариант 5 би осигурил по-голяма ефективност на борбата с кибернетичната престъпност отколкото варианти 3 и 4, като добавя оперативни функции за подпомагане на правоприлагащите и съдебните органи.

3.12 Вариант 5 ще изисква съществено увеличение на ресурсите на Агенцията и отново е свързан с притеснения относно капацитета за усвояване и ефективно използване на бюджета.

3.13 Въпреки че както вариант 4, така и вариант 5 би оказал по-голямо положително въздействие в сравнение с вариант 3, Комисията счита, че има редица причини да не продължава работата по тези варианти:

— Те биха били политически чувствителни за държавите-членки във връзка с техните отговорности по отношение на CIIP (т.е. някои държави-членки не биха подкрепили централизирани оперативни функции).

— Разгледаното във варианти 4 и 5 удължаване на мандата може да придаде двусмислие на позицията на Агенцията.

— Добавянето на тези нови и коренно различни задачи с оперативен характер към мандата на Агенцията може да се окаже много голямо предизвикателство в краткосрочен план и съществува значителен риск Агенцията да не се справи успешно с подобна задача в разумен срок.

— Не на последно място, разходите за изпълнение на варианти 4 и 5 са прекомерно високи - изискваният бюджет би надвишил четирикратно или петкратно настоящия бюджет на ENISA.

([5]) Позоваването на повече ресурси е свързано с условието предложението за ENISA да бъде одобрено в сегашния му вид.

4. **Разпоредби на регламента**

4.1 Агенцията подпомага Комисията и държавите-членки в спазването на правните и регулаторни изисквания на мрежовата и информационна сигурност.

4.2 Управителният съвет определя общата насока на дейността на Агенцията.

4.3 Съставът на Управителния съвет включва по един представител на всяка държава-членка, трима представители, назначени от Комисията и по един представител на отрасъла на информационните и комуникационните технологии, потребителските групи и академични експерти по информационни технологии.

4.4 Агенцията се ръководи от независим изпълнителен директор, който отговаря за изготвянето на работната програма на Агенцията, която се одобрява от Управителния съвет.

4.5 Изпълнителният директор отговаря също за изготвянето на годишния бюджет за изпълнение на работната програма. Управителният съвет представя бюджета и работната програма за одобрение от Комисията и държавите-членки.

4.6 Управителният съвет учредява, по предложение на изпълнителния директор, Постоянна група на заинтересовани страни, съставена от експерти от отрасъла на информационните и комуникационните технологии, потребителски групи, академични експерти и органите за правоприлагане и защита на неприкосновеността на личния живот.

4.7 Тъй като регламентът е все още на етап предложение, съществува известна неяснота по отношение на числовите стойности. Понастоящем Агенцията има персонал от 44-50 души и бюджет от 8 милиона евро. От теоретична гледна точка вариант 3 може да включва състав от 99 души и бюджет от 17 милиона евро.

4.8 В регламента се предлага фиксиран мандат от пет години.

Брюксел, 17 февруари 2011 г.

Председател
на Европейския икономически и социален комитет
Staffan NILSSON