H4 33074 PE Европейска програма за изследвания и иновации в областта на сигурността

КОМИСИЯ НА ЕВРОПЕЙСКИТЕ ОБЩНОСТИ

Брюксел, 21.12.2009
COM(2009)691 окончателен

СЪОБЩЕНИЕ НА КОМИСИЯТА

„Европейска програма за изследвания и иновации в областта на сигурността — първоначална позиция на Комисията относно ключовите констатации и препоръки на Европейския форум за изследвания и иновации в областта на сигурността“

EN

СЪОБЩЕНИЕ НА КОМИСИЯТА

„Европейска програма за изследвания и иновации в областта на сигурността — първоначална позиция на Комисията относно ключовите констатации и препоръки на Европейския форум за изследвания и иновации в областта на сигурността“

1. ВЪВЕДЕНИЕ

Една от основните цели на Европейския съюз е опазването и развитието на европейските ценности на правосъдие, свобода и сигурност, като същевременно не се пренебрегват все по-сложните предизвикателства в областта на сигурността.

В нашето ежедневие нараства значението на борбата против тероризма и организираната престъпност, защитата на външните европейски граници и управлението на граждански кризи. Ако не бъдат предприети подходящи мерки по отношение на изменението на климата, то може да има много сериозни последици за стабилността в световен мащаб. В същото време вътрешната и външната сигурност са в нарастваща степен неделими. И в двете области предприемането на действия изисква използването на модерна технология.

Тъй като все по-осезаемото присъствие на технологиите за сигурност в модерните общества понякога поражда неспокойствие у гражданите, е задължително да се осигури етичен преглед и прозрачност на изследователските и развойни проекти в областта на сигурността. Нашата сигурност трябва да се основава на нашите европейски ценности. И обратно, за защитата на нашите обществени ценности са необходими решения в областта на сигурността.

За да се отговори на тази загриженост през идните години, ще бъде необходимо по-добро разбиране на взаимодействието между човешките и природните фактори, които могат да представляват рискове за сигурността. Това заедно с използването на модерна технология и новаторски решения често има решаващо значение за намирането на ефективен отговор.

Комисията стигна до заключението, че за да бъдат намерени най-ефективните решения на тези предизвикателства, задължително условие е да бъдат събрани заедно представители на промишлеността, публичните и частните крайни потребители, изследователските институти и университетите, както и неправителствените организации и органите на ЕС. Ето защо през 2007 г. тя заедно с държавите-членки предложи учредяването на „Европейски форум за изследвания и иновации в областта на сигурността“ (ЕФИИС)[1].

На него беше възложено създаването на „Програма за изследвания и иновации в областта на сигурността“ за ЕС: стратегически план за изследванията и иновациите в областта на сигурността, с който се цели внасянето на по-голяма последователност и

[1] COM (2007) 511 окончателен.

ефикасност в тази област на равнището на ЕС и на национално и регионално равнище. Освен изследователската и развойната дейност, в центъра на вниманието на програмата са иновациите, на които е отредено откроряващо се място в европейския дневен ред. Нейната насоченост към иновациите и използването на технологиите за сигурност се оказа още по-важна в настоящия световен контекст на глобални екологични и икономически предизвикателства.

На 23 ноември ЕФИИС прие своите ключови констатации и препоръки (за повече информация относно ЕФИИС и неговия подход — вж. също приложеното резюме на окончателния доклад на ЕФИИС).

Настоящото съобщение представлява **първоначалният отговор на Комисията на ключовите констатации и препоръки на ЕФИИС**.

2. ОБЩЕСТВЕНО ИЗМЕРЕНИЕ НА СИГУРНОСТТА

ЕФИИС с право основава своя подход към изследванията в областта на сигурността на виждането, че сигурността е преди всичко човешка и обществена. Хората са не само цели и жертви на атаки и заплахи за сигурността, но също така и спасителите, лицата, които вземат решения, и тези, които противодействат при ситуации на несигурност.

За да бъдат преодолени тези предизвикателства, всички решения в областта на сигурността трябва да се основават на европейските ценности на свобода и правосъдие, на основните етични принципи и на правните изисквания, които са неразделна част от всички изследователски, развойни и иновационни дейности в областта на сигурността. Това означава:

а) Укрепване на правното и етичното измерение

Не могат да съществуват мерки за сигурност, без да се вземе предвид зачитането на правата и свободите на личността, особено защитата на правото на личен живот на гражданите. Мерките за сигурност трябва да бъдат законни и пропорционални, за да спечелят общественото одобрение, както и винаги прилагани в съответствие с върховенството на закона. Основните етични принципи и изискванията за защита на данните на мерките за сигурност трябва да бъдат в основата на разработването и изпълнението на програми за сигурност. ЕФИИС защитава позицията, че изискванията, свързани с правото на личен живот, трябва да присъстват заедно с изискванията за повишена сигурност от най-ранния етап на разглеждане на нови решения в областта на сигурността. Това се нарича „правото на личен живот още при проектирането“.

Този приветстван от Комисията подход ще има дълбоки последици за целия цикъл на изследвания и иновации.

б) Укрепване на общественото измерение

Още едно обществено измерение трябва да бъде взето предвид от гледна точка на ефективността на технологиите. Фактически в дългосрочен план нито една технология в областта на сигурността не може да бъде решение на проблеми на сигурността без активното участие (и приемане от страна) на широката общественост. ЕФИИС всъщност твърди, че подходът на обществената сигурност е свързан с виждане за сигурността, което не се съсредоточава върху превенцията и защитата на всяка цена, а

по-скоро върху способността на нашите общества да се изправят пред рискове, а понякога и загуби, както и да преодоляват понесените поражения. Тази „издръжливост на обществото“ е в еднаква степен зависима от свободната воля на информираните граждани и от качеството на техническите системи и капацитета на дружествата и администрациите за продължаване на дейността.

За да бъде постигната тази издръжливост, са необходими конкретни програми, които да достигат до широката общественост, да повишават осведомеността относно заплахи, да подобряват разбирането на съществуващите механизми за преодоляване на предизвикателствата, както и да служат за обсъждане на приемливостта на решенията в областта на сигурността. Приоритетни са конкретните инициативи с участието на медиите. В съответствие с доклада на ЕФИИС са необходими допълнителни изследвания на отношението между новите технологии и гражданските и човешките права.

3. ПОДОБРЯВАНЕ НА КОНКУРЕНТОСПОСОБНОСТТА НА ЕВРОПЕЙСКАТА ИНДУСТРИЯ НА СИГУРНОСТТА

Европейската индустрия на сигурността, за чиято пазарна стойност през 2008 г. оценката варираще между 26 и 36 милиарда евро[2], показва бърз растеж и се отличава с висококвалифицирана работна сила, като изследователската и развойната дейност е силно представена. ЕФИИС препоръчва като цел изграждането на „солидна и независима технологична и научна база, която да позволи на ЕС да защитава интересите на гражданите и да гарантира, че промишлеността е в състояние да предоставя конкурентоспособни продукти и услуги“. Форумът отправя препоръката ЕС да се стреми да заеме ръководна роля на пазара в областта на сигурността и дава одобрението си за идеята за инициатива за „водещ пазар“ в отрасъла на сигурността.

Това налага обаче да се инвестира сега в амбициозна промишлена политика за отрасъла на сигурността, която в бъдеще да даде плодове във вид на иновации и растеж.

а) Преодоляване на фрагментираността на пазара

Необходимо е европейската индустрия на сигурността да стане по-конкурентоспособна и ефективна. Досега промишлеността страдаше от фрагментираността на пазарите, последица от която е тяхната национална или дори регионална насоченост. Малкият им размер доведе до неефикасност и ниска ефективност на разходите за промишлеността и крайните потребители. Това е значително препятствие пред оперативната съвместимост и интеграцията на решения в областта на сигурността на национално и европейско равнище. Преодоляването на този проблем посредством създаването на европейски пазари ще направи тази промишленост по-конкурентоспособна и по-привлекателна в световен мащаб и ще доведе до по-голяма ефективност на публичните разходи.

---

[2] Индустрията на сигурността обхваща традиционната промишленост в областта на сигурността (основаваща се на доставянето на общи приложения за сигурност, като например контрол на физическия достъп), насочената към сигурността отбранителна промишленост (основаваща се на използването на отбранителни технологии в приложения за сигурност или на придобиването и конверсията на граждански технологии за приложения за сигурност), както и нови участници, т.е. главно дружества, които разширяват своите (граждански) технологии, така че да включват и приложения за сигурност, като например дружествата за информационни технологии.

i) Сертифициране, валидиране и стандартизация

Необходимо е новите технологии и решения да бъдат не само валидирани въз основа на изискванията на крайните потребители и резултатите от научните изследвания, а трябва също да бъдат сертифицирани и, когато е целесъобразно, стандартизирани, така че да могат да станат част от ефективния отговор на заплахите за сигурността. Изследователските и развойните дейности следва да бъдат свързани с ясна стратегия за валидиране и обществени поръчки, в която са взети предвид както съответните проблеми на политиката в областта, така и икономическите интереси. В областта на сигурността това следва да поощри създаването на европейски пазар и по-доброто сътрудничество на заинтересованите страни на национално и на европейско равнище. ЕФИИС препоръчва Комисията да оцени приложимостта и ефикасността на евентуален „Европейски знак за сигурност“.

CEN и ETSI[3] започнаха работа по стандартизацията в областта на сигурността. Първоначално работата на CEN е съсредоточена върху определен брой въпроси, за които комитетът е получил мандат за стандартизация (по-специално сигурност на веригата за доставки, защита на критичната инфраструктура и осигуряване на защита на продукти срещу престъпни посегателства). Тъй като стандартите могат да бъдат ефективно средство за реализиране на резултатите от изследванията в иновативни продукти, очаква се работата, извършена по линия на Седмата рамкова програма, да доведе до по-нататъшна стандартизация. Необходимо е тази дейност да бъде ускорена.

Междувременно Комисията проучва начините, по които резултатите от съответните изследователски дейности биха могли да бъдат изпитвани с оглед разработването на бъдещи механизми на сертифициране. Тези механизми следва да бъдат насочени към сертифицирането на съответствието на продуктите и процесите в областта на сигурността със съществуващите стандарти.

ii) Регулаторна уредба

ЕФИИС подчерта, че предвид фрагментираността на пазара в областта на сигурността, дължаща се често на различаващото се национално законодателство, в конкретни области е препоръчително създаването на хармонизирана регулаторна рамка, съчетана със сътрудничество на по-високо равнище. Комисията счита това за първа стъпка, като е необходим обстоен анализ на съществуващата регулаторна уредба.

iii) Оперативна съвместимост

Споделянето на ресурси и информация засилва нашата способност да работим по комплексни и трансгранични въпроси на сигурността. В борбата против трансграничната престъпност от жизненоважно значение е обменът на информация между националните органи и другите европейски действащи лица. Към днешна дата обаче обменът и споделянето на информация са

[3] http://www.cen.eu/CENORM/sectors/sectors/security+and+defence/security/index.asp
http://www.etsi.org/WebSite/Technologies/Security.aspx

възпрепятствани от липсата на техническа и организационна съвместимост. По тази причина е налице спешна нужда от разработване на стандарти за оперативна съвместимост.

б) Укрепване на промишлената база

Европейският съюз се нуждае от мощна промишлена и технологична база, за да предостави на гражданите на ЕС и държавите извън Съюза модерни решения в областта на сигурността. За да се укрепи европейската промишлена и технологична база в областта на сигурността, трябва да се предприемат действия по следните въпроси:

i) Очертаване на промишлената база в областта на сигурността

За да се получи точна картина на европейската промишлена и технологична база в областта на сигурността, е от значение да се направи карта на съответните компетентности. Това ще позволи да бъдат установени силните и слабите страни на европейската промишлена и технологична база в областта на сигурността, както и подходящите мерки за укрепването ѝ. Следва да се обърне специално внимание на МСП. Също така трябва да бъдат откроени „критичните производствени“ отрасли (като например производство на електрическо оборудване и др.), които играят в производството роля, подобна на тази на критичната инфраструктура в областта на инфраструктурата.

ii) Политика в областта на иновациите

В центъра на вниманието на политиката в областта на иновациите е превръщането на познанието в нови продукти и методи, които в същото време имат икономическа стойност и представляват търговски успех[4]. Това е в сила особено за изследователската и развойната дейност в областта на сигурността. Поради това Комисията ще анализира до каква степен отраслите на сигурността с най-изявен иновационен характер следва да бъдат включени в инициативата за „водещ пазар“.

Освен това полезен инструмент за поощряване на доставките на иновационни продукти и технологии са обществените доставки на развойни продукти[5]. Комисията ще анализира допълнително как да ускори обществените доставки на развойни продукти в сферата на сигурността. По отношение на обществените доставки Директива 2009/81/ЕО[6] се прилага в еднаква степен за доставките на военно и на чувствително оборудване. Комисията ще предложи начини, с които да се гарантира прозрачното и хармонизирано прилагане на тази директива в сферата на сигурността.

iii) Сигурност още при проектирането

ЕФИИС препоръчва „поощряването на подхода за вземане предвид *сигурността още при проектирането* при всяка новоразработена комплексна

4 COM(2005) 488 окончателен.
5 COM(2007) 799 окончателен.
6 ОВ L 216, 20.8.2009 г.

система или продукт, за да се гарантира, че за сигурността се мисли още в идейния стадий, подобно на *безопасността още при проектирането*“.

Комисията приветства тази препоръка и ще проучи начините да се гарантира, когато е целесъобразно, че в научноизследователските дейности с потенциални последици за сигурността тези фактори се вземат под внимание още на най-ранен етап.

iv) Синергии между гражданските и отбранителните технологии

Развиващият се характер на отношението между отбранителните технологии, от една страна, и технологиите в областта на сигурността, от друга, е особено забележим в областта на научноизследователската и развойна дейност, където са налице технологии, които показват потенциал за развитие и в двете области.

Налице е необходимост да се засили допълняемостта и сътрудничеството в конкретни области, в които технологиите могат да имат граждански и отбранителни приложения, включително в областите на граничния контрол и кибернетичната сигурност. Въз основа на призива, получил одобрението на Европейския съвет през декември 2008 г., за по-нататъшно засилване на синергиите между дейностите, провеждани по линията на рамковата програма за научни изследвания и развойна дейност, и тези в сферата на отбраната е необходимо да се обезпечи тясно сътрудничество с Европейската агенция по отбрана (EDA).

4. ИНВЕСТИРАНЕ В БЪДЕЩЕТО

В своята „Европейска програма за изследвания и иновации в областта на сигурността“ ЕФИИС е представил план за изследователската и развойната дейност в областта на сигурността за следващите 15 години, включително и системни изисквания. Необходимо е да се прави разлика между мерките, свързани с изследователската и развойната дейност, и мерките, целящи да гарантират, че постигнатият чрез тази дейност напредък в технологиите ще доведе до действителното внедряване на тези нови технологии.

a) Задачи и приоритети на изследователската и развойната дейност в областта на сигурността

По отношение на изследователската и развойната дейност ЕФИИС подчерта, че за непосредственото бъдеще продължават да бъдат актуални основните изследвания в подкрепа на задачите в областта на сигурността, определени съгласно Седмата рамкова програма. В по-дългосрочен план е необходимо те да бъдат оценени отново и вероятно задълбочени и разширени.

ЕФИИС подчерта, че не е възможно да се предскажат напълно заплахите за сигурността на Европа, независимо дали са дело на човека или са с природен произход. Поради това изследователската и развойната дейност в областта на сигурността трябва да бъде насочена главно към укрепване на издръжливостта на Европа на заплахи и нейната способност за ефективно възстановяване от кризи. Това включва също така повишаването на сплотеността и крепкостта на обществените системи, както и тяхното взаимодействие с технологиите. В този контекст ЕФИИС препоръча, че е необходимо

задълбочаване и разширяване на изследванията на защитата на критичната инфраструктура, например по отношение на изследванията на енергийната сигурност и сигурността на транспортната мрежа[7].

i) Развиващи се приоритети

Европейската програма за изследвания и иновации в областта на сигурността покрива целия спектър на подкрепата за изследователската и развойната дейност за текущите задачи в областта на сигурността. Тя съдържа пет подгрупи (вж. „Обобщение на ЕФИИС“ в приложението).

Комисията отбелязва значението, отдадено от ЕФИИС, на характерния за цялата програма интегрален подход. Независимо дали се отнася до взривни вещества или химични, биологични, радиологични и ядрени инциденти, до критични инфраструктури или управление на кризи, в центъра на вниманието на Европейската програма за изследвания и иновации в областта на сигурността е по-скоро цялото, отколкото частите, като особено се изтъква значението на мрежите, референтните центрове, оперативната съвместимост и решенията, почиващи на системното интегриране на системи. ЕФИИС препоръчва например подготовка „за посрещане на прогнозните нужди от общоевропейски, базиран на информационни мрежи капацитет и комплексни системи за ранно предупреждение и готовност за ответни действия по отношение на природни и причинени от човека инциденти“.

Форумът се застъпва за иновации в подкрепа на „цялостен подход“ при управлението на границите, което фактически беше разработено от ЕС и неговите държави-членки в шенгенския модел на контрол на достъпа на четири нива[8], който представлява ядрото на интегрираното управление на границите. ЕФИИС изтъква значението на оперативната съвместимост, като смята, че „изследванията трябва да обхванат техническите аспекти на оперативната съвместимост на внедрените системи, както и оперативната съвместимост на организационно ниво, като се взема предвид разнообразието на трансграничните култури. Оперативната съвместимост може да бъде повишена и посредством хармонизирани или общи оперативни процедури за разработка, придобиване и обучение“.

Форумът смята, че информационните и комуникационните технологии са „от решаващо значение за европейската сигурност, тъй като те представляват критични инфраструктури сами по себе си, а също така предоставят възможности, на които другите услуги и отрасли разчитат“, като по-специално посочва необходимостта от изследвания за повишаване на издръжливостта на системите. ЕФИИС се застъпва за изследвания на правните уредби в подкрепа на събирането на доказателствен материал в средата, създадена от информационните и комуникационните технологии.

---

[7] Вж. също свързаната с това Директива 2008/114/ЕО на Съвета.

[8] Четирите нива са: мерки в трети държави, сътрудничество със съседни държави, управление на граничния контрол, мерки за контрол в рамките на пространството за свободно движение, в т.ч. връщане.

ЕФИИС определи ролята на космоса като „жизненоважна в различните сфери на технологията, свързани със сигурността“ и посочи значението на Глобалния мониторинг на околната среда и сигурност (GMES) и Галилео за предоставянето на „широк обхват от услуги с добавена стойност в подкрепа на сигурността“, като посочва необходимостта от защита на космическите средства.

Комисията приветства цялостния подход към изследванията и иновациите в областта на сигурността.

ii) Бъдещи задачи

Няколко от задачите в областта на сигурността, които бяха анализирани от ЕФИИС по отношение на необходимия за тях капацитет и свързаните изследователски усилия, са предмет на активно разглеждане. Това се отнася *inter alia* за управлението и контрола на границите, защитата на критичната инфраструктура, включително на информационните и комуникационните технологии, политиката за сигурност относно химични, биологични, радиологични и ядрени инциденти, мерките за увеличаване безопасността на взривните вещества и детонаторите или скрининга на стоки и пътници. Тези области на сигурността ще бъдат допълнително определени в бъдещия Стокхолмски план за действие.

Предизвикателствата за сигурността на информационните и комуникационните технологии представляват част от областите на различни политики и по отношение на тях съответно трябва да се действа в контекста на структурата на информационната система за бъдещата стратегия на ЕС за вътрешна сигурност.

ЕФИИС признава, че неговият мандат не е включвал някои изследователски теми, чието значение неминуемо ще нараства в идните години. Това се отнася по-специално до някои задачи в областта на външната сигурност. ЕФИИС препоръчва „даването на специален приоритет на външното измерение на сигурността“, като има предвид, че: „Програмите за изследвания и иновации следва да подкрепят мироопазващите, хуманитарни и свързаните с управление на кризи задачи, включително общите инициативи с други региони и международни организации, по-специално по отношение разработването на световни стандарти“.

Комисията смята, че макар това наистина да са сфери в процес на развитие, е целесъобразно да се задълбочи обмислянето на въпроса за разширяване на програмите за изследователска и развойна дейност в областта на сигурността, за да бъдат обхванати области като гражданската защита, предотвратяването на конфликти и възстановяването на стабилността след криза.

– Гражданска защита: има предпоставки за нарастване на значението на гражданската защита и съответно изследванията в областта на сигурността за укрепване на гражданската защита, не на последно място в светлината на изменението на климата, както е посочено в работен документ на върховния представител и на Европейската комисия за Европейския съвет, в който

изменението на климата е описано като „умножител на заплахите“[9]. В документа се призовава за увеличаване на капацитета на изследвания на равнището на ЕС по отношение на връзката между сигурността и изменението на климата. Освен това в своето „Съобщение относно повишаване на способността на Съюза за отговор при бедствия“ Комисията подчерта необходимостта от подобряване на предотвратяването на бедствия, смекчаването на техните последици и капацитета на европейската гражданска защита за ответни действия, както и ценната подкрепа, която може да бъде предоставена от научните изследвания;

– Предотвратяване на конфликти и възстановяване на стабилността след криза: Общността вече разполага с оперативно финансиране посредством Инструмента за стабилност[10]. С него се цели установяването или възстановяването на условия, които са от съществено значение за правилното прилагане на политиките на Общността за развитие в случай на криза или възникването на криза, както и да се спомогне за изграждането на капацитет за противодействие на конкретни глобални или трансрегионалните заплахи и да се обезпечи изграждането предкризисна и следкризисна готовност. На равнището на Общността обаче липсва финансиране на изследванията в подкрепа на тези дейности.

б) Отвъд изследователската и развойната дейност

i) Участие на крайните потребители

Макар да препоръчва „*тясно сътрудничество в цяла Европа* между заинтересованите страни сред доставчиците, закупчиците и крайните потребители по отношение на всички цикли на планиране, изпълнение и преглед на политиките относно изследванията в областта на сигурността“, ЕФИИС посочи необходимостта правителствата и крайните потребители да предприемат „адаптиране на организационно равнище с цел даването на форма и на отговор на иновациите в областта на сигурността“.

Комисията е съгласна, че често съществува необходимост от допълнителни усилия от страна както на публичните, така и на частните крайни потребители за укрепване на тяхната база от знания относно технологиите за сигурност и на капацитета им за вероятностен анализ, за да бъдат в състояние напълно да се възползват от възможността да гарантират, че бъдещите решения ще бъдат конкретно съобразени с техните действителни нужди, например чрез демонстрационни модели.

ii) Бъдещи програми за разпространение на иновационни решения

Комисията вече указа ползата от инвестиции в оперативните аспекти на сигурността, по-специално по отношение на редица области, в които националните и международните органи използват технологични решения[11].

---

9 Вж. 7249/08, 3.3.2008 г. Вж. също Съобщение на Комисията относно повишаване на способността на Съюза за отговор при бедствия (COM(2008) 130 окончателен).

10 Регламент (ЕО) № 1717/2006 (ОВ L 327, стр. 1, 24.11.2006 г.).

11 COM (2008) 68 окончателен, COM (2008) 130 окончателен, COM(2009) 262 окончателен.

ЕФИИС смята, че успехът на световния пазар е силно зависим от правилата за доставки на пазара на ЕС и препоръчва да бъде използвана възможността за доставки на развойни продукти, почиващи на иновационни решения.

ЕФИИС подкрепя разработването на модел, основан на стратегически и координиран подход към трансевропейското сътрудничество. Форумът посочва трансевропейските мрежи като пример за това, какво следва да бъде разглеждано като еталон за системна интеграция на равнището на ЕС в областта на сигурността. Както и при трансевропейските мрежи, предоставеното финансиране ще бъде в допълнение на националните средства, изразходвани за сигурността на европейската критична инфраструктура. Като взема предвид, че наличните ресурси за научни изследвания и технологично развитие трябва да бъдат мобилизирани за да се отговори напълно на очакванията на потребителите, ЕФИИС отбеляза, че този процес може да бъде подкрепен със създаването на фонда за вътрешна сигурност.

iii) Образование и обучение

ЕФИИС изтъкна значението на свързването на научното образование и обучение, като счита това за отговорност на всички заинтересовани страни: служители в областта на сигурността, създателите на политиките, агенции по правоприлагането, гражданското общество, промишлеността, изследователските организации, академичния свят и медиите. Форумът се застъпва за нови програми за повишаване на осведомеността, насочени към широката общественост, с цел по-голяма осведоменост относно заплахите, рисковете и уязвимостта, както и по-добро разбиране на необходимите с оглед сигурността политики и технологични решения.

5. ПРИЛАГАНЕ НА ЕВРОПЕЙСКАТА ПРОГРАМА ЗА ИЗСЛЕДВАНИЯ И ИНОВАЦИИ В ОБЛАСТТА НА СИГУРНОСТТА

В препоръките на ЕФИИС относно управлението се разглеждат начините за актуализиране на програмата и за обезпечаване на по-тясно участие на всички имащи отношение заинтересовани лица. ЕФИИС препоръчва *създаването на прозрачен механизъм с участието на всички заинтересовани лица за балансирано и стриктно прилагане на Европейската програма за изследвания и иновации в областта на сигурността*.

Тъй като изследванията в областта на сигурността са насочени към потребителя и се основават на капацитета, ЕФИИС отбелязва необходимостта от адекватни механизми за взаимодействие и обмен между общността на крайните потребители, изследователската общност и промишлеността.

6. ЗАКЛЮЧЕНИЕ

Настоящото е предварителен отговор на Комисията на окончателния доклад на ЕФИИС. Комисията смята за важни резултатите от работата на ЕФИИС и приветства нейната стратегическа насоченост. Комисията отбелязва препоръките на Форума и подчертава следните теми, които е възможно следващата Комисия да пожелае да анализира допълнително:

- ролята на Агенцията на Европейския съюз за основните права[12,13] за предприемането на изследвания относно взаимовръзките между сигурността, личния живот и защитата на данните;

- необходимостта от задълбочаване на „етичния преглед“ на проектите, разглеждани по темата „Сигурност“ в Седмата рамкова програма (FP7), и осигуряване на възможно най-широк достъп до резултатите от текущите изследователски и развойни проекти в областта на сигурността.

- общественото измерение като очаквано същностно въздействие във всички покани за предложения по темата „Сигурност“ в Седмата рамкова програма (FP7);

- възможността за включването на отраслите на сигурността с най-изявен иновационен характер в инициативата за „водещ пазар“;

- как да бъдат ускорени обществените доставки на развойни продукти в сферата на сигурността;

- начините за ускоряване на работата по сертифицирането, валидирането и, по целесъобразност, стандартизацията в областта на сигурността, по-специално относно приложимостта и ефикасността на евентуален „Европейски знак за сигурност“;

- намирането на най-успешните отговори на предвидими нови задачи и приоритети в областта на сигурността, или в контекста на настоящата Седма рамкова програма, или при изготвянето на бъдещата рамкова програма;

- начините за по-добро свързване на равнището на ЕС и на държавите-членки на европейската изследователска и развойна дейност с по-голям брой оперативни аспекти на сигурността;

- установяването на постоянно работеща структура за изпълнението на препоръките на ЕФИИС;

- с цел увеличаване на конкурентоспособността на индустрията на сигурността възможността за учредяването на форум, който да развива дейност в полето на изследователската и развойната дейност, като например „група на високо равнище“ с участието на всички заинтересовани страни от публичния и частния сектор, като и от гражданското общество.

---

12 Решение № 2008/203/ЕО на Съвета (ОВ L 63, 7.3.2008 г.).

13 Регламент № 168/2007, ОВ L 53, 22.2.2007 г.

Annex: Executive Summary of the ESRIF Final Report

Europe stands on the threshold of a new global approach to security – and of ways to use scientific research and innovation to reinforce and implement that new thinking

The security of Europe and its citizens is linked to internal and external events and threats, as well as to the increasing convergence of civil and defence capabilities. Above all, it derives from societal imperatives that demand a balancing of the state's policy and technological exigencies with privacy rights, European cultural values and the tenets of democracy.

ESRIF, the European Security Research and Innovation Forum, has spent the past two years analyzing the medium and long-term challenges that Europe faces. These range from natural disasters to organised crime to man-made incidents, whether small-scale in impact or those with potential "mass disruption" effects.

Assisted by more than 600 experts, ESRIF and its 64 members from 31 countries have examined the full range of such threats and tied them to the EU's central civil security missions and to the capabilities required to carry them out.

This collective effort has resulted in a set of key messages that encompass the logic and necessity of future European security and its related research. These messages point to the essence, as ESRIF sees it, of what security research and innovation should flow from – and what it should deliver to society.

Security research should be grounded in an industrial policy that frames a systematic approach to capability development which, in turn, promotes interoperability among the 27 EU nations and establishes common standards. Ultimately this effort must increase societal security in a globalised world, while fostering trust between European citizens, governments and national and European institutions. These and other ideas are among ESRIF's main recommendations included in this executive summary.

To reach an interoperable, trust-embedded and resilient society, however, Europe needs an R&D roadmap, and a mechanism should be set up to implement it in a balanced and rigorous manner. ESRIF thus proposes its European Security Research and Innovation Agenda – "ESRIA" which should go a long way toward achieving that goal.

A research and innovation agenda cannot be created and implemented in a vacuum.

The framework is defined by principles given in the **Key Messages**:

- **Societal Security**

  Human beings are at the core of security processes.

- **Societal Resilience**

  Certain risks cannot be catered for, nor avoided. Societies must prepare to face shocks and must have the ability to recover.

- **Trust**

Assuring security implies nurturing trust among people, institutions and technologies.

- **Awareness raising through education and training**

  Security is a common responsibility of all stakeholders, the citizen is at the fore front.

- **Innovation**

  Europe can only rely on its own scientific, technological and industrial competences.

- **Industrial policy**

  A competitive European security industry is a prerequisite for future security. The EU must address the fragmentation of its security markets.

- **Interoperability**

  A seamless approach to security is essential for Europe; Interoperability is essential to allow security forces to work together.

- **A systematic approach to capability development**

  The increasing complexity of security, demands increasing sophistication of our Response.

- **Security by design**

  Security features must become integral part of any given system: Europe's society needs a systemic approach to security.

ESRIF has defined a **European Security Research and Innovation Agenda** (ESRIA) that identifies and roadmaps key capabilities and research needs in line with the main work results.

The ESRIA has been organized into **five content clusters** and differentiates research topics according to short-, medium- or long-term needs:

- The first cluster centres on the classic event cycle of prevention, protection, preparing, responding and recovering. It focuses on the securing of people, civil preparedness and crisis management.

- The second cluster deals with the countering of different means of attack, as a way of dealing with specific, known and projected future risks. It examines ways to detect and identify conventional as well as non-conventional attacks, unintended impacts of other actions, and naturally occurring incidents, to mitigate their effects, and it analyzes potential dangers inherent to coming technologies.

- The third cluster aims at securing critical assets, such as energy, transport and other crucial infrastructures. It examines security economics and outlines the necessity to analyze and cope with limited access to critical natural resources as well as securing the existence of key manufacturing capabilities and capacities in Europe.

- The fourth cluster is about securing identity, access and movement of people and goods. It mainly centres on border security and secure identity management.

- Lastly, the fifth cluster lists additional enabling capabilities of special interest, due to cross-cutting characteristics or prior political strategic decisions. The crucial role of Information and Communication Technologies (ICT) is examined, as are security implications of European space programmes.

ESRIF strongly recommends that the EU and its Member States launch new measures to enhance the security of its citizens. These should also aim to create amenable conditions for European excellence in research and innovation, and thus advance Europe's security. The below sets out policy and operational recommendations for achieving stronger security research and innovation results:

COMMON EUROPEAN CAPABILITIES

The EU must draw on its collective strengths and knowledge by developing common capability via enhanced transnational co-operation.

1. This calls for *close consultation across Europe* among supply, demand and end-user stakeholders across the planning, execution and review cycles of security research policy. The demand side in particular – governments and end-users – needs organisational re-alignment to both shape and respond to security innovation.

2. *Resources and incentives* are essential to developing common capability. ESRIF recommends, notably with a view to the implementation of ESRIA, that the EU maintains the current rate of growth of its security research programmes – with the aim of reaching an annual budget of one billion euros as proposed in 2004 by the Group of Personalities. National programmes should reflect this degree of ambition. Regarding the necessary research and industrial synergies, technical compatibility and interoperability of new security solutions, a significant effort is required to ensure the coherence of national and EU efforts through enhanced coordination.

3. Research programmes should be complemented by additional implementation programmes. Success on the global market strongly depends on EU market procurement references. Pre-commercial procurement of innovative solutions should be exploited as a mechanism to bring research results closer to the market.

NEW POLICY INITIATIVES

The above should be supported by stronger articulation of demand, and delivery of the most appropriate solutions by the supply side.

4. New initiatives and programmes should include:

   – creation of knowledge centres such as CBRN expert groups to guide research

– preparations to meet foreseeable needs for pan-European network-enabled capabilities and complex systems in early warning and response readiness that deal with natural and man made incidents

– expanded critical infrastructure protection programmes

– evaluating the applicability and efficacy of the numerous initiatives available to the EU and its Members States such as: a Lead Market initiative, Trans European Networks for Security, the creation of an Internal Security Fund or a "European Security Label".

– the early engagement of all stakeholders and transparency of the regulatory environment, including standards to stimulate private sector investments in security research. If upcoming regulations are understood early on, a return on security investments can be foreseen and investments can thus be expected to take place.

INTEGRATED APPROACH TO SECURITY

Effective civil security must embrace interoperability, standardisation, certification, validation, communication with the public, education & training, exchange of best practices, consultations on privacy issues and other factors that cut across public and private spheres and provide synergies between civil security and defence research fields.

5. A *holistic approach* must include:

– efforts to ensure that the social, cultural, legal and political aspects of security research and development are taken into account. Research programmes should reflect relevant ESRIF key messages, and thus promote overall "societal coherence".

– the promotion of a *security by design* approach in any newly developed complex system or product, ensuring that security is addressed at the point of conception, as it has been the case for *safety by design*.

– programmes to raise societal awareness of security threats, risks and vulnerabilities – and the security and safety impact of emerging critical technologies.

THE GLOBAL DIMENSION

The EU's civil security is a collective responsibility touching government, societal organisations, industry and individual citizens. It cannot stand in isolation from the world.

6. The globally inter-related nature of security calls for:

– a strong and independent technological and scientific base for the EU to safeguard the interests of its citizens and ensure that its industry is able to provide products and services in a competitive manner.

– giving high priority to security's external dimension and closer home affairs/defence consultation. Research and innovation programmes should support peacekeeping, humanitarian and crisis management tasks, including joint initiatives with other regions and international organisations, notably as regard the development of global standards.

SECURITY RESEARCH: THE FUTURE

The proposed European Security Research and Innovation Agenda – ESRIA – should be seen as a living document.

7. For *ESRIA to evolve* with Europe's internal and external threat environments:

– A transparent mechanism involving all stakeholders should be set up to implement ESRIA in a balanced and rigorous manner.

– ESRIA should be revisited and evaluated on a regular basis with special attention to evaluating any measures flowing from ESRIF key messages.