H4 33074 PE Europese agenda voor onderzoek en innovatie

COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN

Brussel, 21.12.2009
COM(2009)691 definitief

MEDEDELING VAN DE COMMISSIE

Een Europese agenda voor onderzoek en innovatie op het gebied van veiligheid – Initieel standpunt van de Commissie over de belangrijkste bevindingen en aanbevelingen van het ESRIF

EN

MEDEDELING VAN DE COMMISSIE

Een Europese agenda voor onderzoek en innovatie op het gebied van veiligheid – Initieel standpunt van de Commissie over de belangrijkste bevindingen en aanbevelingen van het ESRIF

1. INLEIDING

Een van de hoofddoelstellingen van de EU bestaat erin de Europese waarden van rechtvaardigheid, vrijheid en veiligheid te behoeden en te bevorderen en tegelijkertijd de steeds complexere veiligheidsproblemen aan te pakken.

De strijd tegen terrorisme en georganiseerde misdaad, de bescherming van de Europese buitengrenzen en civiele crisisbeheersing zijn in ons dagelijks leven steeds belangrijker geworden. Als de klimaatverandering niet adequaat wordt aangepakt, zal dit wereldwijd ingrijpende destabiliserende gevolgen hebben. Tegelijkertijd raken interne en externe veiligheid steeds meer met elkaar vervlochten. Om de interne en externe veiligheid te waarborgen, moet moderne technologie worden gebruikt.

Nu veiligheidstechnologieën steeds nadrukkelijker in onze moderne samenlevingen aanwezig zijn en soms de bezorgdheid van de burgers wekken, is het noodzakelijk onderzoeks- en ontwikkelingsprojecten op het gebied van veiligheid aan grondig ethisch toezicht te onderwerpen en de transparantie ervan te waarborgen. Onze veiligheid moet op onze Europese waarden gebaseerd zijn. Omgekeerd moet naar veiligheidsoplossingen worden gezocht om onze maatschappelijke waarden te beschermen.

Om deze problemen de komende jaren aan te pakken, is beter inzicht nodig in de wisselwerking tussen menselijke en natuurlijke factoren die veiligheidsrisico's kunnen creëren. Een beter inzicht is – naast het gebruik van moderne technologieën en innovatieve oplossingen – ook van cruciaal belang om de uitdagingen doeltreffend aan te gaan.

De Commissie achtte het noodzakelijk vertegenwoordigers van het bedrijfsleven en van publieke en particuliere eindgebruikers, onderzoeksinstellingen en universiteiten, niet-gouvernementele organisaties en EU-organen samen te brengen om de meest doeltreffende oplossingen voor deze uitdagingen te vinden. Daarom heeft de Commissie in 2007 samen met de lidstaten voorgesteld het Europees Forum voor onderzoek en innovatie op het gebied van veiligheid (ESRIF) op te richten[1].

Het forum kreeg de opdracht een "agenda voor onderzoek en innovatie op het gebied van veiligheid" voor de EU te ontwikkelen: een strategisch stappenplan voor onderzoek en innovatie op het gebied van veiligheid die tot meer coherentie en efficiëntie leidt en het Europese, nationale en regionale niveau omvat. Het forum schenkt niet alleen aandacht aan onderzoek en ontwikkeling, maar kent ook aan innovatie een plaats toe in de Europese agenda. De gerichtheid op innovatie en de toepassing van veiligheidstechnologieën bleek

[1] COM(2007) 511 definitief.

zelfs nog belangrijker in het kader van de huidige wereldwijde economische en milieuproblemen.

Op 23 november heeft het ESRIF zijn belangrijkste bevindingen en aanbevelingen goedgekeurd (de bijgevoegde samenvatting van het ESRIF-eindverslag bevat nadere informatie over het ESRIF en de gevolgde aanpak).

Deze mededeling bevat het **initiële standpunt van de Commissie over de belangrijkste bevindingen en aanbevelingen van het ESRIF**.

2. DE MAATSCHAPPELIJKE DIMENSIE VAN VEILIGHEID

Het ESRIF is er bij de benadering van veiligheidsonderzoek terecht van uitgegaan dat veiligheid op de allereerste plaats een menselijke en maatschappelijke dimensie heeft. Mensen zijn niet alleen het doelwit en het slachtoffer van aanslagen en bedreigingen van de veiligheid, maar zij zijn ook de reddingswerkers, de besluitvormers en degenen die op onveilige situaties reageren.

Om deze uitdagingen aan te gaan, moeten alle veiligheidsoplossingen op de Europese waarden van vrijheid en rechtvaardigheid worden gebaseerd en moeten fundamentele ethische beginselen en wettelijke voorschriften in alle O&O- en innovatieactiviteiten op het gebied van veiligheid worden geïntegreerd. Dit omvat twee dimensies:

a) De wettelijke en ethische dimensie versterken

Bij veiligheidsmaatregelen moeten de rechten en vrijheden van de burgers – en vooral de bescherming van hun privacy – in acht worden genomen. Veiligheidsmaatregelen moeten legitiem en evenredig zijn om maatschappelijk te worden aanvaard en altijd in overeenstemming met de rechtsstaat worden toegepast. Fundamentele ethische beginselen en voorschriften inzake gegevensbescherming moeten de basis vormen voor de ontwikkeling en toepassing van veiligheidsprogramma's. Het ESRIF vindt dat bij het concipiëren van nieuwe veiligheidsoplossingen de voorschriften ter verbetering van de veiligheid vanaf het allereerste begin gepaard moeten gaan met privacyvoorschriften. Het ESRIF noemt dit "privacy by design".

De Commissie verwelkomt deze aanpak, die diepgaande gevolgen zal hebben voor de hele onderzoeks- en innovatiecyclus.

b) De maatschappelijke dimensie versterken

Met het oog op de doeltreffendheid van de technologieën moet nog met een andere maatschappelijke dimensie rekening worden gehouden. Geen enkele veiligheidstechnologie kan een oplossing op lange termijn bieden zonder de actieve participatie van (en de aanvaarding door) het grote publiek. Volgens het ESRIF impliceert een maatschappelijke benadering van veiligheid een visie op veiligheid die niet op preventie en bescherming tot elke prijs is geconcentreerd, maar die eerder uitgaat van het vermogen van onze samenlevingen om gevaren – en soms verliezen – onder ogen te zien, maar er ook weer bovenop te komen. Deze "maatschappelijke veerkracht" hangt evenveel af van de vrije wil van geïnformeerde burgers als van de kwaliteit van technische systemen en van de capaciteit van bedrijven en overheidsdiensten hun activiteiten voort te zetten.

Om te zorgen voor maatschappelijke veerkracht is er behoefte aan specifieke programma's om de bevolking over gevaren voor te lichten, haar meer inzicht te bieden in de processen om uitdagingen het hoofd te bieden en de aanvaardbaarheid van veiligheidsoplossingen met haar te bespreken. Er moet prioriteit worden verleend aan specifieke initiatieven via de media. Overeenkomstig het ESRIF-verslag moet verder onderzoek worden verricht naar het verband tussen nieuwe technologieën en burger- en mensenrechten.

3. HET CONCURRENTIEVERMOGEN VAN DE EUROPESE VEILIGHEIDSINDUSTRIE VERBETEREN

De Europese veiligheidsindustrie had in 2008 een marktwaarde van naar schatting 26 à 36 miljard euro[2], groeit snel en beschikt over hooggekwalificeerde werknemers en een hoog O&O-gehalte. Het ESRIF beveelt de EU aan naar een "sterke en onafhankelijke technologische en wetenschappelijke basis voor de EU te streven om de belangen van de Europese burgers te vrijwaren en ervoor te zorgen dat de Europese industrie op concurrerende wijze producten kan leveren en diensten verlenen". Verder beveelt het ESRIF de EU aan naar een leidende rol op de veiligheidsmarkt te streven en pleit het voor een initiatief voor leidende markten in de veiligheidssector.

Daartoe moet echter nu in een ambitieus industrieel beleid voor de veiligheidssector worden geïnvesteerd, zodat morgen innovatie en groei kunnen worden geoogst.

a) Een einde maken aan de versnippering van de markt

De Europese veiligheidsindustrie moet concurrerender en efficiënter worden. Tot dusver leed de bedrijfstak onder de versnippering van de markt, waardoor bedrijven nationaal of zelfs regionaal georiënteerd waren. Hun kleine omvang leidde tot inefficiëntie en een lage kosteneffectiviteit voor zowel de industrie als de eindgebruikers. De versnippering van de markt is een belangrijk obstakel voor de interoperabiliteit en de integratie van veiligheidsoplossingen op nationaal en Europees vlak. Door het probleem aan te pakken en Europawijde markten te creëren, is het mogelijk de veiligheidsindustrie op wereldvlak concurrerender en aantrekkelijker te maken en overheidsmiddelen efficiënter te gebruiken.

i) Certificering, validering en normalisering

Rekening houdend met de eisen van de eindgebruikers en de onderzoeksresultaten moeten nieuwe technologieën en oplossingen niet alleen worden gevalideerd, maar ook gecertificeerd en zo nodig genormaliseerd, zodat zij deel kunnen uitmaken van een doeltreffende respons op gevaren voor de veiligheid. O&O-activiteiten zouden gekoppeld moeten worden aan een duidelijke validerings- en inkoopstrategie die rekening houdt met de relevante beleidsthema's en de economische belangen. Hierdoor kan de totstandkoming van een Europese veiligheidsmarkt en een betere samenwerking tussen de nationale en Europese belanghebbenden op

[2] De veiligheidsindustrie omvat de traditional veiligheidsindustrie (gebaseerd op het leveren van algemene veiligheidstoepassingen zoals toegangsbewaking), de op veiligheid gerichte defensie-industrie (gebaseerd op het gebruik van defensietechnologieën in veiligheidstoepassingen of het verwerven en converteren van civiele technologieën in veiligheidstoepassingen) en nieuwkomers op de markt, d.w.z. voornamelijk bedrijven (bijvoorbeeld IT-bedrijven) die hun bestaande (civiele) technologieën uitbreiden tot veiligheidstoepassingen.

veiligheidsgebied worden bevorderd. Het ESRIF beveelt de Commissie aan de haalbaarheid en de doeltreffendheid van een "Europees veiligheidslabel" te bestuderen.

CEN en ETSI[3] werken nu aan veiligheidsnormen. CEN schenkt in eerste instantie vooral aandacht aan een aantal kwesties waarvoor het een mandaat heeft gekregen (met name normalisatie op het gebied van de veiligheid van de toeleveringsketen, de bescherming van kritieke infrastructuur en de beveiliging van producten tegen misdrijven). Aangezien normen een doeltreffend middel kunnen zijn om onderzoeksresultaten in innovatieve producten te integreren, wordt verwacht dat de werkzaamheden in het kader van het zevende kaderprogramma – die versneld moeten worden uitgevoerd – tot verdere normalisering zullen leiden.

Ondertussen gaat de Commissie na hoe de resultaten van relevant onderzoek getest kunnen worden met het oog op de ontwikkeling van toekomstige certificeringsmechanismen. Deze mechanismen zijn bedoeld om te certificeren dat veiligheidsproducten en -processen in overeenstemming zijn met de desbetreffende normen.

ii) Regelgevingskader

Gezien de versnippering van de veiligheidsmarkt – vaak als gevolg van onderling verschillende nationale wetgevingen – heeft het ESRIF beklemtoond dat een geharmoniseerd regelgevingskader voor specifieke gebieden in combinatie met voorafgaande coördinatie raadzaam is. De Commissie is van oordeel dat er om te beginnen behoefte is aan een grondige analyse van het bestaande regelgevingskader.

iii) Interoperabiliteit

Door een gezamenlijk gebruik van een technisch instrumentarium en van informatie kunnen wij complexe en grensoverschrijdende veiligheidskwesties beter aanpakken. De uitwisseling van informatie tussen nationale autoriteiten en andere Europese actoren is van vitaal belang voor de strijd tegen grensoverschrijdende criminaliteit. Het uitwisselen en delen van informatie wordt momenteel echter gehinderd door een gebrek aan technische en organisatorische interoperabiliteit. Daarom moeten dringend interoperabiliteitsnormen worden ontwikkeld.

b) De industriële basis versterken

De Europese Unie heeft een sterke industriële en technologische basis nodig om de burgers in de EU en daarbuiten van moderne veiligheidsoplossingen te voorzien. De volgende kwesties moeten worden aangepakt om de Europese industriële en technologische basis op veiligheidsgebied te versterken:

i) De industriële basis van veiligheid in kaart brengen

Om een duidelijk beeld te krijgen van de Europese technologische en industriële basis van veiligheid (European Security Technological and Industrial Base - ESTIB)

---

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

is het belangrijk deze competenties in kaart te brengen. Zo kunnen de sterke en zwakke punten van de ESTIB worden geïdentificeerd en passende maatregelen worden genomen om de ESTIB te versterken. Bijzondere aandacht moet worden besteed aan het midden- en kleinbedrijf, evenals aan "kritieke productiesectoren" (bijvoorbeeld de productie van elektrische apparatuur), die een soortgelijke rol spelen als kritieke infrastructuur in de wereld van de infrastructuur.

ii) Innovatiebeleid

Innovatiebeleid beoogt kennis om te zetten in nieuwe producten en methoden en tegelijkertijd ook in economische waarde en commercieel succes[4]. Dit is bijzonder relevant voor O&O op het gebied van veiligheid. De Commissie zal daarom nagaan in hoever de meest innovatieve veiligheidssectoren bij het initiatief voor leidende markten moeten worden betrokken.

Verder is precommerciële inkoop een nuttig instrument om de inkoop van innovatieve producten en technologieën te bevorderen[5]. De Commissie zal verder onderzoeken hoe precommerciële inkoop op het gebied van veiligheid kan worden versneld. Wat overheidsopdrachten betreft, is Richtlijn 2009/81/EG[6] ook van toepassing op defensie-uitrusting en gevoelige apparatuur. De Commissie zal voorstellen doen om ervoor te zorgen dat deze richtlijn op transparante en geharmoniseerde wijze in de veiligheidssector wordt toegepast.

iii) Veiligheid door ontwerp

Het ESRIF beveelt "de bevordering aan van een op *security by design* gebaseerde aanpak bij elk nieuw ontwikkeld complex systeem of product, zodat – naar analogie van *safety by design* – vanaf het ontwerp met de veiligheid rekening wordt gehouden".

De Commissie verwelkomt deze aanbeveling en zal nagaan hoe – waar nodig – gewaarborgd kan worden dat bij onderzoeksactiviteiten met potentiële veiligheidseffecten vanaf het beginstadium met deze effecten rekening wordt gehouden.

iv) Synergieën tussen civiele en defensietechnologieën

De zich voortdurend ontwikkelende verhouding tussen defensietechnologieën enerzijds en veiligheidstechnologieën anderzijds is vooral zichtbaar op het gebied van O&O in de vorm van technologieën met potentiële ontwikkelingen op beide gebieden.

De complementariteit en de samenwerking moeten worden versterkt op specifieke gebieden waar technologieën civiele en defensietoepassingen kunnen hebben, onder meer op het gebied van grenstoezicht en cyberveiligheid. Op basis van een door de Europese Raad van december 2008 onderschreven oproep om de synergieën tussen activiteiten in het kader van het O&O-programma en de defensiesector te versterken,

---

4 COM(2005) 488 definitief.
5 COM(2007) 799 definitief.
6 PB L 216 van 20.8.2009.

moet worden gezorgd voor een nauwe samenwerking met het Europees Defensieagentschap (EDA).

4. INVESTEREN IN DE TOEKOMST

Het ESRIF heeft in de Europese agenda voor onderzoek en innovatie op het gebied van veiligheid een stappenplan voor O&O op het gebied van veiligheid voor de volgende 15 jaar opgenomen (inclusief systemische vereisten). Er moet een onderscheid worden gemaakt tussen O&O-maatregelen en maatregelen die bewerkstelligen dat dankzij O&O geboekte technologische vooruitgang daadwerkelijk leidt tot de toepassing van die nieuwe technologie:

a) O&O-taken en -prioriteiten op het gebied van veiligheid

Wat O&O betreft wijst het ESRIF erop dat het belangrijkste onderzoek ter ondersteuning van de in het zevende kaderprogramma geïdentificeerde veiligheidstaken in de nabije toekomst geldig blijft. Op lange termijn moeten zij opnieuw worden geëvalueerd en mogelijk worden versterkt en uitgebreid.

Het ESRIF beklemtoont dat het onmogelijk is alle gevaren voor de veiligheid van Europa als gevolg van menselijke activiteiten of natuurlijke processen te voorspellen. Daarom moet het O&O op het gebied van veiligheid er vooral naar streven de veerkracht van Europa ten aanzien van gevaren te versterken, evenals het vermogen om zich doeltreffend van crises te herstellen. Dit houdt onder meer in dat de samenhang en het weerstandsvermogen van maatschappelijke systemen en hun interface met technologieën moeten worden versterkt. Het ESRIF beveelt in dit verband aan het onderzoek naar de bescherming van kritieke infrastructuur te versterken en uit te breiden (bijvoorbeeld het onderzoek naar energiezekerheid en de veiligheid van transportnetwerken)[7].

i) Veranderende prioriteiten

De Europese agenda voor onderzoek en innovatie op het gebied van veiligheid bestrijkt het volledige spectrum van O&O-ondersteuning voor bestaande veiligheidstaken en bestaat uit vijf clusters (zie de samenvatting van het ESRIF in de bijlage).

De Commissie merkt op dat het ESRIF overal in de agenda de nadruk legt op een integratieve aanpak. De agenda beklemtoont met betrekking tot explosieven, CBRN, kritieke infrastructuur en crisisbeheer het geheel eerder dan de onderdelen en benadrukt het belang van netwerken, referentiecentra, interoperabiliteit en system-of-systems solutions. Het ESRIF beveelt bijvoorbeeld aan voorbereidingen te treffen "om te voldoen aan te verwachten behoeften aan pan-Europese netwerkgebaseerde capaciteiten en complexe systemen op het gebied van vroegtijdige waarschuwing en snelle reactie bij incidenten als gevolg van menselijke activiteiten of natuurlijke processen".

Het ESRIF pleit voor innovatie ter ondersteuning van een "holistische aanpak" van grensbeheer. De EU en de lidstaten hebben overigens een dergelijke aanpak

[7] Zie ook Richtlijn 2008/114/EG van de Raad.

ontwikkeld in het vierledige toegangscontrolemodel van Schengen[8], dat de kern vormt van het geïntegreerd grensbeheer. Het ESRIF benadrukt het belang van interoperabiliteit aangezien "het onderzoek aandacht moet schenken aan de technische interoperabiliteit van opgestelde systemen en aan organisatorische interoperabiliteit zonder de verscheidenheid van grensoverschrijdende culturen uit het oog te verliezen. De interoperabiliteit kan ook worden versterkt door geharmoniseerde of gemeenschappelijke operationele procedures voor ontwikkeling, inkoop en opleiding".

Het ESRIF vindt dat informatie- en communicatietechnologieën "van cruciaal belang zijn voor de Europese veiligheid omdat zij zelf tot de kritieke infrastructuur behoren en als basis voor andere diensten en sectoren fungeren" en benadrukt met name de behoefte aan onderzoek om de systemische veerkracht te vergroten. Het ESRIF pleit voor onderzoek naar rechtskaders ter ondersteuning van forensisch onderzoek en het verzamelen van bewijsmateriaal in de ICT-omgeving.

Volgens het ESRIF speelt de ruimte een "vitale rol op verschillende technologische gebieden die met veiligheid verband houden". Het ESRIF wijst ook op het belang van GMES en Galileo die "een groot aantal diensten met een meerwaarde ter ondersteuning van de veiligheid verlenen" en beklemtoont dat ruimtematerieel beschermd moet worden.

De Commissie verwelkomt deze alomvattende benadering van onderzoek en innovatie op het gebied van veiligheid.

ii) Toekomstige taken

Verschillende veiligheidstaken die door het ESRIF werden geanalyseerd uit het oogpunt van vereiste capaciteiten en onderzoeksinspanningen worden momenteel nader onder de loep genomen. Dat is onder meer het geval voor grensbeheer en -toezicht, bescherming van kritieke infrastructuur, inclusief ICT, het CBRN-veiligheidsbeleid, maatregelen ter verbetering van de veiligheid van explosieven en detonators en de screening van goederen en passagiers. Deze veiligheidsgebieden zullen nader worden gedefinieerd in het toekomstige actieplan van Stockholm.

ICT-veiligheidsproblemen zijn in verschillende beleidsgebieden aan de orde en moeten dienovereenkomstig worden aangepakt in het kader van de informatiesysteemarchitectuur voor de toekomstige interneveiligheidsstrategie van de EU.

Het ESRIF erkent dat onderzoeksthema's die de komende jaren zeker aan belang zullen winnen (met name een aantal aspecten van externe veiligheid) niet onder zijn mandaat vielen. Het ESRIF beveelt daarom aan "topprioriteit te verlenen aan de externe dimensie van veiligheid" aangezien "onderzoeks- en innovatieprogramma's steun zouden moeten verlenen aan vredeshandhaving, humanitaire hulp en crisisbeheer, met inbegrip van gezamenlijke initiatieven met andere regio's en internationale organisaties, met name bij de ontwikkeling van mondiale normen".

---

[8] Het vierledige toegangscontrolemodel omvat maatregelen in derde landen, samenwerking met buurlanden, grenstoezicht en controlemaatregelen binnen de ruimte van vrij verkeer, met inbegrip van terugkeer.

Aangezien er zich op deze gebieden voortdurend veranderingen voordoen, acht de Commissie het raadzaam grondiger na te denken over de verruiming van de O&O-programma's op het gebied van veiligheid tot gebieden als civiele bescherming, conflictpreventie en stabiliserende maatregelen in post-crisissituaties.

– Civiele bescherming: de civiele bescherming en vandaar ook het veiligheidsonderzoek ter ondersteuning van de civiele bescherming zullen wellicht aan belang winnen, niet in het minst in het licht van de klimaatverandering. Dat is het oordeel van de Hoge Vertegenwoordiger en de Europese Commissie in een verslag aan de Europese Raad, waarin de klimaatverandering wordt beschreven als een "verveelvoudiging van de bedreigingen"[9]. In het verslag wordt ervoor gepleit de onderzoekscapaciteiten van de EU met betrekking tot het verband tussen veiligheid en klimaatverandering te versterken. Bovendien beklemtoont de Commissie in haar mededeling "Versterking van het reactievermogen van de Unie bij rampen" dat het zaak is de preventie van rampen, de leniging van de gevolgen ervan en het Europese reactievermogen op het gebied van civiele bescherming te verbeteren en dat onderzoek daarbij waardevolle steun kan bieden.

– Conflictpreventie en stabiliserende maatregelen in post-crisissituaties: de Gemeenschap zorgt ook nu al voor operationele financiering via het stabiliteitsinstrument[10]. Het instrument wil in een situatie van crisis of dreigende crisis de noodzakelijke voorwaarden voor een behoorlijke uitvoering van het EU-ontwikkelingsbeleid creëren of herstellen, de capaciteit om specifieke mondiale en transregionale bedreigingen aan te pakken helpen opbouwen en de paraatheid waarborgen om met pre- en post-crisissituaties te kunnen omgaan. Het ontbreekt op EU-niveau echter aan financiële middelen om deze activiteiten te ondersteunen.

b) Andere aspecten dan onderzoek en ontwikkeling

i) Betrokkenheid van eindgebruikers

Het ESRIF beveelt "*nauw overleg in heel Europa* tussen belanghebbenden op het gebied van vraag, aanbod en eindgebruik aan tijdens de plannings-, uitvoerings- en evaluatiecycli van het beleid inzake veiligheidsonderzoek" en heeft vastgesteld dat regeringen en eindgebruikers "een organisatorische herschikking moeten doorvoeren om vorm te geven aan en te reageren op veiligheidsinnovatie".

De Commissie is het ermee eens dat particuliere en openbare veiligheidseindgebruikers vaak een extra inspanning moeten leveren om hun kennisbasis inzake veiligheidstechnologie en hun toekomstige analysecapaciteiten te versterken om ervoor te zorgen dat toekomstige oplossingen op hun reële behoeften zijn toegesneden (bijvoorbeeld via demonstratiemodellen).

ii) Toekomstige programma's om innovatieve oplossingen te verspreiden

---

9 Zie 7249/08 van 3.3.2008. Zie ook de mededeling van de Commissie "Versterking van het reactievermogen van de Unie bij rampen" (COM(2008) 130 definitief.

10 Verordening (EG) nr. 1717/2006, PB L 327 van 24.11.2006, blz. 1.

De Commissie heeft al te kennen gegeven dat het zinvol is in de operationele aspecten van veiligheid te investeren, met name voor een aantal gebieden waar nationale en internationale autoriteiten technologische oplossingen aanwenden[11]. Het ESRIF vindt dat het succes op de wereldmarkt sterk van de EU-referenties voor overheidsopdrachten afhangt en beveelt aan de precommerciële inkoop van innovatieve oplossingen te benutten.

Het ESRIF steunt de ontwikkeling van een model dat gebaseerd is op een strategische en gecoördineerde benadering van trans-Europese samenwerking. Het verwijst naar de trans-Europese netwerken als een voorbeeld dat als referentiepunt kan dienen voor de Europawijde systemische integratie in de ruimte van veiligheid. Zoals voor de TEN's zou financiering worden verstrekt ter aanvulling van nationale middelen om Europese kritieke infrastructuur te beveiligen. Aangezien de beschikbare middelen voor onderzoek en technologische ontwikkeling gebruikt moeten worden om ten volle aan de verwachtingen van de gebruikers te voldoen, merkt het ESRIF op dat een dergelijk proces ondersteund kan worden door de oprichting van een fonds voor interne veiligheid.

iii) Onderwijs en opleiding

Het ESRIF beklemtoont dat het belangrijk is onderzoek aan onderwijs en opleiding te koppelen en dat alle belanghebbenden (veiligheidsbeamten, beleidsmakers, rechtshandhavingsinstanties, maatschappelijke organisaties, het bedrijfsleven, onderzoeksorganisaties, de academische wereld en de media) op dat gebied hun verantwoordelijkheid moeten nemen. Het ESRIF pleit voor nieuwe voorlichtingsprogramma's voor het grote publiek om de aandacht op gevaren, risico's en kwetsbare punten te vestigen en het inzicht in beleidsmaatregelen en de voor veiligheid vereiste technologische oplossingen te vergroten.

5. UITVOERING VAN DE EUROPESE AGENDA VOOR ONDERZOEK EN INNOVATIE OP HET GEBIED VAN VEILIGHEID

De aanbevelingen van het ESRIF inzake governance houden verband met de vraag hoe de agenda up-to-date kan worden gehouden en hoe alle belanghebbenden nauwer bij de agenda kunnen worden betrokken. Het ESRIF beveelt aan *een transparant mechanisme met alle belanghebbenden op te zetten om de agenda evenwichtig en rigoureus uit te voeren*.

Gezien het gebruikersgerichte en capaciteitengestuurde karakter van veiligheidsonderzoek is er volgens het ESRIF behoefte aan adequate interfaces en uitwisselingsmechanismen tussen de eindgebruikers, de onderzoekers en het bedrijfsleven.

6. CONCLUSIE

Dit is een eerste reactie van de Commissie op het ESRIF-eindverslag. De Commissie acht de resultaten van de ESRIF-activiteiten belangrijk en is het eens met de strategische oriëntatie ervan. Zij neemt nota van de aanbevelingen in het verslag en benadrukt de volgende punten die de volgende Commissie wellicht grondiger kan analyseren:

[11] COM(2008) 68 definitief, COM(2008) 130 definitief, COM(2009) 262 definitief.

- de rol van het Bureau van de Europese Unie voor de grondrechten[12] [13] om onderzoek te doen naar het verband tussen veiligheid, privéleven en gegevensbescherming;

- de noodzaak om het "ethisch toezicht" op projecten in het kader van het thema veiligheid van het zevende kaderprogramma te versterken en de resultaten van lopende O&O-projecten op het gebied van veiligheid zo toegankelijk mogelijk te maken;

- de maatschappelijke dimensie als een inherent verwacht effect van alle oproepen tot het indienen van voorstellen rond het thema veiligheid van het zevende kaderprogramma;

- de mogelijkheid om de meest innovatieve veiligheidssectoren bij het initiatief voor leidende markten te betrekken;

- de wijze waarop precommerciële inkoop op het gebied van veiligheid kan versnellen;

- methoden om de activiteiten inzake certificering, validering en – zo nodig – normalisering op het gebied van veiligheid te versnellen, met name wat de toepasbaarheid en doeltreffendheid van een Europees veiligheidslabel betreft;

- de wijze waarop zij – in het kader van het lopende zevende kaderprogramma of bij de voorbereiding van het toekomstige kaderprogramma – het best kan reageren op nieuwe veiligheidstaken en -prioriteiten in de nabije toekomst;

- de wijze waarop Europees O&O op het gebied van veiligheid op nationaal en EU-niveau beter kan worden gekoppeld aan meer operationele aspecten van veiligheid;

- de totstandbrenging van een permanente werkstructuur voor de uitvoering van de ESRIF-aanbevelingen;

- de mogelijkheid om een forum op te richten ter versterking van het concurrentievermogen van de veiligheidsindustrie die zich bezighoudt met onderzoek en innovatie, zoals een groep op hoog niveau waarin de belanghebbenden van de overheid, de privésector en het maatschappelijk middenveld vertegenwoordigd zijn.

---

[12] Besluit 2008/203/EG van de Raad, PB L 63 van 7.3.2008.

[13] Verordening (EG) nr. 168/2007, PB L 53 van 22.2.2007.

Annex: 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.