KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER

Bruxelles, den 21.12.2009
KOM(2009)691 endelig

MEDDELELSE FRA KOMMISSIONEN

"En europæisk sikkerhedsforsknings- og innovationsdagsorden - Kommissionens første bemærkninger til ESRIF's vigtigste resultater og anbefalinger"

EN

MEDDELELSE FRA KOMMISSIONEN

"En europæisk sikkerhedsforsknings- og innovationsdagsorden - Kommissionens første bemærkninger til ESRIF's vigtigste resultater og anbefalinger"

1. INDLEDNING

Et af EU's vigtigste mål er at bevare og udvikle de europæiske værdier for retfærdighed, frihed og sikkerhed samtidig med at håndtere de stadig mere komplekse sikkerhedspolitiske udfordringer.

Kampen mod terrorisme og organiseret kriminalitet, beskyttelsen af de ydre europæiske grænser og civil krisestyring har fået større betydning i vores daglige liv. Klimaændringer vil, hvis der ikke gøres noget, kunne føre til større destabiliserende virkning på globalt plan. Samtidig er indre og ydre sikkerhed i stigende grad uadskillelige. Løsning af dem kræver brug af moderne teknologi.

Da sikkerhedsteknologier bliver mere og mere nærværende i det moderne samfund, forekommer der til tider udtryk for bekymring herover hos en del af borgerne, og det er derfor bydende nødvendigt at sikre etisk kontrol og gennemsigtighed i sikkerhedsforsknings- og -udviklingsprojekter. Vores sikkerhed må være baseret på vores europæiske værdier. Og omvendt er sikkerhedsløsninger nødvendige for at beskytte vores samfundsmæssige værdier.

Håndtering af disse problemer i de kommende år vil kræve en bedre forståelse af samspillet mellem de menneskelige og naturlige faktorer, som kan medføre sikkerhedsrisici, som ofte også er afgørende for at forme en effektiv indsats sammen med brugen af moderne teknologi og innovative løsninger.

Kommissionen mente, at det for at finde de mest effektive løsninger på disse udfordringer var nødvendigt at samle repræsentanter fra erhvervslivet, offentlige og private slutbrugere, forskningsinstitutioner og universiteter, samt ikke-statslige organisationer og EU-organer. I 2007 foreslog den derfor, sammen med medlemsstaterne, oprettelsen af Det Europæiske Forum for Forskning og Innovation på Sikkerhedsområdet - ESRIF[1].

ESRIF blev pålagt at udvikle en "sikkerhedsforsknings- og innovationsdagsorden" (ESRIA) for EU: en strategisk plan for sikkerhed, forskning og innovation, der sigter mod at skabe større sammenhæng og effektivitet på dette område, der omfatter EU, nationalt og regionalt plan. Den fokuserer ud over forskning og udvikling på at sætte "I" for innovation på den europæiske dagsorden. Dens orientering mod innovation og implementering af sikkerhedsteknologi viste sig at være endnu mere vigtigt i den nuværende kontekst af globale miljømæssige og økonomiske udfordringer.

Den 23. november 2009 vedtog ESRIF sine vigtigste resultater og anbefalinger (for mere information om ESRIF og dets tilgang se også vedlagte resumé (EN) af ESRIF's endelige rapport).

---

[1] KOM (2007) 511 endelig

Denne meddelelse indeholder Kommissionens første bemærkninger til **ESRIF's vigtigste resultater og anbefalinger**.

2. DEN SAMFUNDSMÆSSIGE DIMENSION AF SIKKERHED

ESRIF baserede med rette sin tilgang til sikkerhedsforskning på det perspektiv, at sikkerhed først og fremmest har et menneskeligt og et samfundsmæssigt aspekt. Mennesker er ikke kun mål og ofre for overgreb og trusler mod sikkerheden, men også redningsfolk, beslutningstagere og dem, der reagerer på situationer præget af usikkerhed.

For at løse disse udfordringer skal alle sikkerhedsmæssige løsninger være baseret på europæiske værdier som frihed og retfærdighed, og grundlæggende etiske principper og lovkrav skal integreres gennem alle sikkerhedsrelaterede FoU- og innovationsaktiviteter. Det betyder:

a) Styrkelse af den juridiske og etiske dimension

Der kan ikke være sikkerhed uden at tage hensyn til respekten for den enkeltes rettigheder og frihedsrettigheder, især til beskyttelse af borgernes privatliv. Sikkerhedsforanstaltninger skal være legitime og rimelige for at få samfundets accept og altid anvendes i overensstemmelse med retsstatsprincippet. Grundlæggende etiske principper og databeskyttelse af sikkerhedsforanstaltninger skal være fundamentet for at udvikle og gennemføre sikkerhedsprogrammer. ESRIF tilråder, at krav relateret til privatlivets fred bør figurere ligebyrdigt med sikkerhedsforbedringskrav fra de tidligste stadier af behandlingen af nye sikkerhedsløsninger. ESRIF kalder dette for *"privacy by design"* (indbygget databeskyttelse).

En sådan fremgangsmåde, som hilses velkommen af Kommissionen, vil få vidtrækkende konsekvenser for hele forsknings- og innovationscyklussen.

b) Styrkelse af den samfundsmæssige dimension

Der bør tages hensyn til en yderligere samfundsmæssig dimension ud fra teknologiernes effektivitet. Ingen sikkerhedsteknologi kan i virkeligheden på lang sigt være en sikkerhedsløsning uden aktiv deltagelse (og godkendelse) af den brede offentlighed. Faktisk hævder ESRIF, at en samfundsorienteret sikkerhedstilgang bygger på en opfattelse af sikkerhed, som ikke fokuserer på forebyggelse og beskyttelse for enhver pris, men snarere vores samfunds evne til at se risici, og til tider tab, i øjnene og at komme sig igen. En sådan "samfundsmæssig modstandsdygtighed" afhænger lige så meget af informerede borgeres frie vilje som kvaliteten af de tekniske systemer og om virksomheders og forvaltningers evne til forretningskontinuitet.

For at opnå modstandsdygtighed kræves der specifikke programmer, der skal nå ud til den brede offentlighed, som øger bevidstheden om trusler, for at forbedre forståelsen af de processer, der er iværksat for at tackle udfordringer og også til debat om accepten af sikkerhedsløsninger. Konkrete initiativer, der inddrager medierne, er en prioritet. I overensstemmelse med ESRIF-rapporten er yderligere forskning om forholdet mellem nye teknologier og civile rettigheder og menneskerettigheder påkrævet.

3. FORBEDRE KONKURRENCEEVNEN FOR DEN EUROPÆISKE SIKKERHEDSINDUSTRI

Med en anslået markedsværdi i 2008 på mellem 26 og 36 mia. EUR[2] vokser EU's sikkerhedsindustri hurtigt med en højt kvalificeret arbejdsstyrke og et højt FoU-indhold. ESRIF anbefaler, at man stræber mod et "stærkt og uafhængigt teknologisk og videnskabeligt grundlag for EU til at beskytte borgernes interesser og sikre, at industrien er i stand til konkurrencedygtigt at levere varer og tjenester". ESRIF anbefaler, at EU skal nå frem til lederskab i sikkerhedsmarkedet og støtter idéen om et *lead market*-initiativ i sikkerhedssektoren.

Dette kræver dog, at man i dag, med henblik på at høste innovation og vækst i morgen, investerer i en ambitiøs industripolitik for sektoren for sikkerhed:

a) Overvinde markedsfragmentering

Sikkerhedsindustrien i Europa har brug for at blive mere konkurrencedygtig og effektiv. Indtil nu har branchen lidt under opsplitning af markederne, der fører dem til at være nationalt eller endog regionalt orienterede. Den lille størrelse har ført til ineffektivitet og dårlig omkostningseffektivitet både for branchen og slutbrugere. Det er en vigtig hindring for interoperabilitet og integration af sikkerhedsløsninger på nationalt og europæisk plan. Bekæmpelse af problemet ved at oprette et EU-dækkende marked vil gøre branchen mere konkurrencedygtig og attraktiv på globalt plan og føre til mere effektiv anvendelse af offentlige udgifter.

i) Certificering, validering og standardisering

Baseret på kravene fra slutbrugere og resultaterne af forskningen, skal nye teknologier og løsninger ikke blot være validerede, de bør også være certificerede, og evt. standardiserede, så de kan blive en del af et effektivt svar på trusler mod sikkerheden. FoU-aktiviteter bør være knyttet til en klar validerings- og indkøbsstrategi, der tager hensyn til de relevante politiske spørgsmål samt økonomiske interesser. Dette vil fremme etablering af et europæisk sikkerhedsmarked og et bedre samarbejde mellem sikkerhedsinteressenter på nationalt og europæisk plan. ESRIF anbefaler, at Kommissionen bør evaluere anvendeligheden og effekten af et "europæisk sikkerhedsstrategi-mærke".

CEN og ETSI[3] er begyndt at arbejde på standardisering på området for sikkerhed. CEN koncentrerer sig i første omgang om en række spørgsmål, som det har modtaget standardiseringsmandater til (især om sikring af forsyningskæden, beskyttelse af kritisk infrastruktur og sikring af produkter mod kriminalitet). Da standarder kan være et effektivt middel til overførsel af forskningsresultater til innovative produkter, forventes det, at arbejde udført under det 7. rammeprogram vil føre til yderligere standardisering. Dette arbejde skal fremskyndes.

---

2 Sikkerhedsindustrien omfatter den traditionelle sikkerhedsindustri (baseret på levering af generelle sikkerhedsapplikationer som f.eks. fysisk adgangskontrol), sikkerhedsorienteret forsvarsindustri (baseret på udnyttelse af forsvarsteknologi i sikkerhedsapplikationer eller gennem opkøb og ombygning af civile teknologier til sikkerhedsapplikationer), såvel som nye aktører, dvs. primært virksomheder, der udvider deres eksisterende (civile) teknologi til sikkerhedsapplikationer, som for eksempel it-virksomheder.

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

I mellemtiden er Kommissionen ved at undersøge måder, hvorpå resultaterne af relevante forskningsaktiviteter kan afprøves med henblik på at udvikle fremtidige certificeringsmekanismer. Sådanne mekanismer bør sigte på, at det bekræftes, at sikkerhedsprodukter og -processer er i overensstemmelse med relevante standarder.

ii) Regelsæt

ESRIF har understreget, at en harmoniseret ramme på specifikke områder kombineret med forudgående koordinering i betragtning af opsplitningen af sikkerhedsmarkedet, ofte på grund af divergerende nationale lovgivning, ville være tilrådelig. Kommissionen mener, at en grundig analyse af det eksisterende regelsæt som et første skridt er nødvendig.

iii) Interoperabilitet

Deling af aktiver og oplysninger styrker vores evne til at håndtere komplekse og grænseoverskridende sikkerhedsspørgsmål. Udveksling af oplysninger mellem de nationale myndigheder og andre europæiske aktører er afgørende for bekæmpelsen af grænseoverskridende kriminalitet. Men i dag er en sådan udveksling og deling af information hæmmet på grund af mangel på teknisk og organisatorisk interoperabilitet. Der er derfor et presserende behov for udvikling af interoperabilitetsstandarder.

b) Styrkelse af det industrielle grundlag

EU har brug for en stærk industriel og teknologisk base for at kunne tilbyde sine egne borgere og borgere i tredjelande moderne sikkerhedsløsninger. Følgende emner skal behandles med henblik på at styrke det europæiske sikkerhedsindustrielle og -teknologiske grundlag:

i) Kortlægning af sikkerhedsindustriens grundlag

For at få et præcist billede af den europæiske sikkerhedsindustrielle og -teknologiske basis (ESTIB) er det vigtigt at kortlægge disse kompetencer. En sådan kortlægning vil gøre det muligt at identificere styrker og svagheder i ESTIB, og vil gøre det muligt at identificere passende foranstaltninger med henblik på at styrke ESTIB. Særlig opmærksomhed skal rettes mod små og mellemstore virksomheder. "Kritiske" fremstillingssektorer (som for eksempel produktion af elektrisk udstyr osv.) - som spiller en lignende rolle i fremstillingssektoren som kritisk infrastruktur gør i forbindelse med infrastrukturen - bør også fremhæves.

ii) Innovationspolitik

Innovationspolitik fokuserer på omsætning af viden til nye produkter og metoder, og på samme tid til økonomisk værdi og kommerciel succes[4]. Dette er særlig relevant for sikkerheds-FoU. Kommissionen vil derfor undersøge, hvor langt de mest innovative sikkerhedssektorer bør bringes ind i *lead market*-initiativet.

[4] KOM (2005) 488 endelig.

Desuden er prækommercielle indkøb et nyttigt værktøj for at fremme indkøb af innovative produkter og teknologier[5]. Kommissionen vil endvidere undersøge, hvordan man kan fremskynde prækommercielle indkøb på sikkerhedsområdet. Hvad angår offentlige indkøb, gælder direktiv 2009/81/EF[6] også for levering af forsvarsmateriel og følsomt udstyr. Kommissionen vil foreslå måder til at sikre, at dette direktiv anvendes på en gennemsigtig og harmoniseret måde på sikkerhedsområdet.

iii) *Security by design*

ESRIF anbefaler "at man fremmer en *security by design*-tilgang i forbindelse med alle nyudviklede komplekse systemer eller produkter, der sikrer, at der er taget hensyn til sikkerheden allerede på tidspunktet for projektstarten, som det har været tilfældet i forbindelse med *safety by design*".

Kommissionen glæder sig over denne anbefaling og vil undersøge, hvordan man, når det er hensigtsmæssigt, kan sikre, at forskningsaktiviteter med potentielle sikkerhedsvirkninger tager disse i betragtning fra de tidligste stadier.

iv) Synergier mellem civile og militære teknologier

Forholdet mellem forsvarsteknologi på den ene side og sikkerhedsteknologi på den anden side, der hele tiden udvikler sig, er særlig mærkbart inden for FoU, med teknologier, der viser den potentielle udvikling på begge områder.

Der er et behov for at styrke komplementaritet og samarbejde på specifikke områder, hvor teknologier kan have civile og militære anvendelser, herunder grænsekontrol og cybersikkerhed. Baseret på en opfordring, der blev godkendt i december 2008 af Det Europæiske Råd, til yderligere at styrke synergierne mellem aktiviteter, der udføres under FoU-rammeprogrammet og forsvarsdomænet, skal et tæt samarbejde med Det Europæiske Forsvarsagentur (EDA) sikres.

4. INVESTERING I FREMTIDEN

ESRIF har i den europæiske sikkerhedsforsknings- og innovationsdagsorden (ESRIA) fastlagt en sikkerhedsrelateret FoU-køreplan for de næste 15 år, herunder også systemiske krav. Der skal skelnes mellem FoU-foranstaltninger og foranstaltninger med henblik på at sikre, at teknologiske fremskridt gennem FoU fører til en faktisk anvendelse af denne nye teknologi:

a) FoU-sikkerhedsopgaver og -prioriteter

For så vidt angår FoU har ESRIF understreget, at den vigtigste forskning til støtte for sikkerhedsopgaver, der er identificeret under FP7, forbliver gyldig i den nærmeste fremtid. På længere sigt skal de tages op til fornyet overvejelse og eventuelt styrkes og forstærkes.

ESRIF understregede, at det ikke er muligt fuldt ud at forudsige trusler mod Europas sikkerhed, hvad enten de er menneskeskabte eller naturlige. Derfor bør det

[5] KOM (2007) 799 endelig.
[6] EUT L 216 af 20.8.2009.

sikkerhedsrelaterede FoU-behov fokusere på at styrke Europas evne til at modstå trusler og dets evne til effektivt at komme sig efter kriser. Dette omfatter også at styrke sammenhængskraften og robustheden af de samfundsmæssige systemer og deres grænseflade med teknologier. I den forbindelse anbefalede ESRIF, at forskning om beskyttelse af kritisk infrastruktur skal styrkes og forstærkes, for eksempel med hensyn til energisikkerhedsforskning og transportnetsikkerhed[7].

i) Skiftende prioriteter

Den europæiske sikkerhedsforsknings- og innovationsdagsorden dækker hele spektret af FoU-støtte til de nuværende sikkerhedsopgaver. Den er inddelt i fem grupper (se resumé af ESRIF i bilaget (EN)).

Kommissionen noterer sig den vægt, som ESRIF lægger på en integrativ tilgang på tværs af hele ESRIA. Hvad enten der henvises til sprængstoffer eller CBRN, kritisk infrastruktur eller krisestyring, fokuserer ESRIA på det hele i stedet for delene, fokuserende på vigtigheden af netværk, referencecentre, interoperabilitet, og *system-of-system*-løsninger. Faktisk anbefaler ESRIF eksempelvis, at man forbereder sig på at "imødekomme det forventede behov for paneuropæiske netaktiverede funktioner og komplekse systemer i tidlig varslings- og reaktionsparathed, der beskæftiger sig med natur- og menneskeskabte ulykker".

Det slår til lyd for, at innovation udgør grundlaget for en "holistisk tilgang" til forvaltning af grænserne, som faktisk er udviklet af EU og dets medlemsstater i den firestrengede Schengen-adgangskontrolmodel[8], som udgør kernen af den integrerede forvaltning af grænserne. ESRIF fremhæver betydningen af interoperabilitet, og finder, at "forskning skal dække tekniske interoperabilitetsaspekter mellem anvendte systemer, samt interoperabilitet på det organisatoriske plan, under hensyntagen til de forskellige grænseoverskridende kulturer. Interoperabilitet kan også styrkes gennem harmoniserede eller fælles operationelle procedurer for udvikling, indkøb og uddannelse".

ESRIF mener, at informations- og kommunikationsteknologier er af "afgørende betydning for europæisk sikkerhed, da de i sig selv er kritiske infrastrukturer og også katalysatorer, som andre tjenester og sektorer beror på", og henviser især til nødvendigheden af forskning for at øge den systemiske modstandskraft. ESRIF går ind for forskning i juridiske rammer til støtte for retsmedicinsk og anden indsamling af bevismateriale i ikt-miljøet.

ESRIF har identificeret verdensrummets rolle som værende af "afgørende betydning på forskellige sikkerhedsrelaterede teknologiske domæner" og fokuserede på vigtigheden af GMES og Galileo i at give "en bred vifte af værdiforøgende tjenester til støtte for sikkerhed", og henviser til behovet for at beskytte rumaktiviteter.

Kommissionen hilser denne vidtspændende tilgang til sikkerhedsforskning og innovation velkommen.

---

7 Se også Rådets direktiv 2008/114/EF (relateret).

8 De fire lag er: foranstaltninger i tredjelande, samarbejde med nabolande, forvaltning af grænsekontrol og kontrolforanstaltninger inden for området for fri bevægelighed, herunder tilbagesendelse.

ii) Fremtidige missioner

Flere af de sikkerhedsopgaver, som blev analyseret af ESRIF for så vidt angår deres nødvendige kompetencer og beslægtede forskningsindsats er under aktiv behandling i form af udvikling af sikkerhedssituationspolitikken. Dette er bl.a. tilfældet for grænsekontrol og kontrollen af CBRN-sikkerhedspolitikken, foranstaltninger for at øge sikkerheden omkring sprængstoffer og detonatorer eller screening af gods og passagerer. Disse sikkerhedsområder vil yderligere blive defineret i den fremtidige Stockholm-handlingsplan.

Ikt-sikkerhedsmæssige udfordringer hører under i forskellige politikområder og skal blive behandlet i overensstemmelse hermed i forbindelse med informationssystemarkitekturen for det fremtidige EU's indre sikkerhedsstrategi.

ESRIF erkendte, at dets mandat udelukker forskningsspørgsmål, der med sikkerhed vil vokse i betydning i de kommende år. Dette gælder især for nogle eksterne sikkerhedsmissioner. ESRIF anbefalede "at give høj prioritet til sikkerhedens eksterne dimension", da "FoU-programmer bør støtte fredsbevarende, humanitære og krisestyringsopgaver, herunder fælles initiativer med andre regioner og internationale organisationer, navnlig for så vidt angår udviklingen af globale standarder ".

Kommissionen mener, at selv om disse rent faktisk er domæner i udvikling, er det imidlertid hensigtsmæssigt at indlede en debat om udvidelse af sikkerhedsrelaterede FoU-programmer til også at omfatte områder som f.eks. civilbeskyttelse, konfliktforebyggelse og postkrisestabilisering:

– Civilbeskyttelse: Civilbeskyttelse og dermed sikkerhedsforskning til at underbygge civilbeskyttelsesaktiviteter vil få større betydning, ikke mindst i lyset af klimaforandringerne, som beskrevet i et dokument fra den højtstående repræsentant og Europa-Kommissionen til Det Europæiske Råd, hvori klimaændringerne er beskrevet som en "trusselsmultiplikator"[9]. I dokumentet opfordres til en intensivering af EU's forskningskapacitet med hensyn til sammenhængen mellem sikkerhed og klimaændringer. Desuden understregede Kommissionen i sin meddelelse om "Styrkelse af EU's katastrofeberedskab" behovet for at forbedre katastrofeforebyggelse og -afbødning, det europæiske civilbeskyttelsesberedskab, og den værdifulde støtte, som forskningen kan give.

Konfliktforebyggelse og postkrisestabilisering: Via stabilitetsinstrumentet[10] har Fællesskabet allerede operationel finansiering på plads. Det sigter mod at skabe eller genskabe væsentlige betingelser for en korrekt gennemførelse af EU's udviklingspolitik i tilfælde af en krise eller en begyndende krise, samt at bidrage til at opbygge kapacitet til at håndtere specifikke globale og tværregionale trusler, samt sørge for opbygning af et præ- og postkriseberedskab. Imidlertid mangler der forskningsmidler til at støtte disse aktiviteter på EU-plan.

b) Ud over forskning og udvikling

---

9 Se 7249/08 af 3.3.2008. Se også Kommissionens meddelelse *"Climate change and international security"*, KOM(2008) 130 endelig.

10 Forordning (EF) nr. 1717/2006, EUT L 327, s. 1, 24.11.2006.

i) Slutbrugerdeltagelse

Ved at anbefale et "*tæt samråd i hele Europa* mellem udbud, efterspørgsel og slutbrugerinteressenter på tværs af planlægning, gennemførelse og revisionscyklusser af sikkerhedsforskningspolitikken" peger ESRIF på behovet for, at regeringer og slutbrugere skal iværksætte en "organisatorisk gentilpasning med henblik på både at kunne udforme og reagere på sikkerhedsinnovation".

Kommissionen er enig i, at der ofte er behov for en ekstra indsats fra sikkerhedsslutbrugerne, både offentlige og private, til at styrke deres sikkerhedsteknologiske videngrundlag og fremadrettede analyseevner, der skal være i stand til fuldt ud at benytte sig af muligheden for at sikre, at fremtidige løsninger vil blive skræddersyet til deres reelle behov, for eksempel gennem demonstrationsmodeller.

ii) Fremtidige programmer til at udbrede innovative løsninger

Kommissionen har allerede fokuseret på nytten af at investere i de operationelle aspekter af sikkerhed, især for en række områder, hvor nationale og internationale myndigheder bruger teknologiske løsninger[11]. ESRIF mener, at succes på det globale marked i høj grad afhænger af EU-markedets indkøbsreferencer, og anbefaler, at prækommercielle udbud af innovative løsninger bør udnyttes.

ESRIF støtter udvikling af en model baseret på en strategisk og koordineret tilgang til det transeuropæiske samarbejde. ESRIF henviser til de transeuropæiske net som et eksempel, som bør betragtes som en reference for den EU-dækkende systemiske integration på sikkerhedsområdet. Ligesom for de transeuropæiske net vil der blive ydet midler til at supplere nationale midler til at sikre europæisk kritisk infrastruktur. I betragtning af, at midlerne til forskning og teknologisk udvikling skal udnyttes for fuldt ud at svare til brugernes forventninger, bemærkede ESRIF, at "en sådan proces kan understøttes ved at iværksætte en intern sikkerhedsfond".

iii) Uddannelse og videreuddannelse

ESRIF fremhævede betydningen af at knytte forskning, uddannelse og videreuddannelse sammen og anser dette for et ansvar for alle aktører: sikkerhedsansvarlige, politikere, retshåndhævende myndigheder, civilsamfundet, erhvervslivet, forskningsorganisationer, den akademiske verden og medierne. ESRIF anbefaler nye bevidstgørelsesprogrammer, som medtager den bredere offentlighed med henblik på at øge bevidstheden om trusler, risici og sårbarhed og for at forbedre offentlighedens forståelse af politikkerne og de teknologiske løsninger, der kræves for en øget sikkerhed.

5. GENNEMFØRELSE AF DEN EUROPÆISKE SIKKERHEDSFORSKNINGS- OG INNOVATIONSDAGSORDEN

ESRIF's anbefalinger vedrørende de generelle principper ser på, hvordan man kan holde ESRIA aktuel, og hvordan man i højere grad kan inddrage alle relevante parter. ESRIF

[11] KOM(2008) 68 endelig, KOM(2008) 130 endelig, KOM(2009) 262 endelig.

anbefaler, at der bør etableres en gennemsigtig mekanisme, der involverer alle berørte parter, til at gennemføre ESRIA på en afbalanceret og stringent måde.

Da sikkerhedsforskning er brugerorienteret og vidensdrevet bemærker ESRIF, at der er behov for passende grænseflader og mekanismer for udveksling mellem slutbrugersamfundet og det forsknings- og industrielle samfund.

6. KONKLUSION

Dette er en foreløbig reaktion fra Kommissionen på ESRIF's endelige rapport. Kommissionen betragter resultaterne af arbejdet i ESRIF som værende vigtigt og glæder sig over den strategiske orientering. Den noterer sig de i rapporten indeholdte anbefalinger og peger på følgende emner, som den næste Kommission måtte ønske at overveje at analysere yderligere:

- Den rolle, som Den Europæiske Unions Agentur for Grundlæggende Rettigheder[12][13] kan spille ved at udføre forskning vedrørende forholdet mellem sikkerhed og privatlivets fred og databeskyttelse.

- Behovet for at styrke den "etiske kontrol" af projekter, der revideres under sikkerhedstemaet under FP7 og gøre igangværende FoU-projekter og deres resultater på området for sikkerhed så bredt tilgængelige som muligt.

- Indførelse af den samfundsmæssige dimension som en iboende forventet virkning af alle indkaldelser af forslag under FP7-sikkerhedstemaet.

- Mulighederne for, hvor langt de mest innovative sikkerhedssektorer bør bringes ind i lead market-initiativet.

- Mulighederne for at fremme certificerings-, validerings-, og i givet fald, standardiseringsarbejde inden for sikkerhed, især hvad angår anvendeligheden og effekten af et "europæisk sikkerhedsstrategi-mærke".

- Hvordan den bedst kan reagere på logisk kommende nye sikkerhedspolitiske opgaver og prioriteter, enten inden for rammerne af det nuværende FP7, eller som forberedelse til det kommende rammeprogram.

- Mulighederne for en bedre koordination, på EU-plan og i medlemsstaterne, mellem den europæiske sikkerhedsforskning og -udvikling og andre operationelle aspekter af sikkerhed.

- Etablering af en permanent arbejdsstruktur til at gennemføre ESRIF's anbefalinger.

- Muligheden for at etablere et forum til at styrke konkurrenceevnen i den del af sikkerhedsindustrien, der er aktiv inden for forskning og innovation, som en højtstående gruppe med deltagelse af alle aktører, såvel fra den offentlige og private sektor samt civilsamfundet.

---

[12] Rådets afgørelse 2008/203/EF, EUT L 63 af 7.3.2008.

[13] Forordning (EF) nr. 168/2007, EUT L 53 af 22.2.2007.

Annex: ESRIF Executive Summary

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.