**H4 33074 PE European Security Research and Innovation Agenda**

KOMISIJA EVROPSKIH SKUPNOSTI

Bruselj, 21.12.2009
COM(2009)691 konč.

# SPOROČILO KOMISIJE

## „Evropski program za varnostne raziskave in inovacije – prvotno mnenje Komisije o glavnih ugotovitvah in priporočilih ESRIF“

EN

**SPOROČILO KOMISIJE**

**„Evropski program za varnostne raziskave in inovacije – prvotno mnenje Komisije o glavnih ugotovitvah in priporočilih ESRIF“**

## 1. UVOD

Eden glavnih ciljev EU je ohranjati in razvijati evropske vrednote pravice, svobode in varnosti in hkrati obravnavati čedalje bolj zapletene izzive varnosti.

Boj proti terorizmu in organiziranemu kriminalu ter varovanje zunanjih evropskih meja in obvladovanje civilnih kriz sta v vsakdanjem življenju postala pomembnejša. Neustrezen odziv na podnebne spremembe lahko privede do velikih destabilizacijskih učinkov na svetovni ravni. Hkrati postajata notranja in zunanja varnost čedalje bolj neločljivi. Za njuno zagotavljanje je potrebna moderna tehnologija.

Ker varnostne tehnologije čedalje bolj postajajo sestavni del moderne družbe in občasno zbujajo pomisleke pri državljanih, je nujno zagotoviti etično preverjanje in preglednost varnostnih raziskav in razvojnih projektov. Naša varnost mora temeljiti na evropskih vrednotah. Obratno pa so varnostne rešitve potrebne za varstvo naših družbenih vrednot.

Obravnavanje teh vprašanj bo v prihodnjih letih zahtevalo boljše razumevanje medsebojnega vpliva človeških in naravnih dejavnikov, ki so lahko vir tveganj za varnost, poleg tega pa je takšno razumevanje pogosto bistveno za pripravo učinkovitega odziva ob uporabi moderne tehnologije in inovativnih rešitev.

Komisija je menila, da je za najučinkovitejši odziv na te izzive nujno združiti predstavnike industrije, javne in zasebne končne uporabnike, raziskovalne ustanove in univerze ter nevladne organizacije in organe EU. Zato je leta 2007 skupaj z državami članicami predlagala vzpostavitev „evropskega foruma za varnostne raziskave in inovacije“ – ESRIF[1].

Njegova naloga je bila oblikovati „program na področju varnostnih raziskav in inovacij“ za EU: strateški načrt za varnostne raziskave in inovacije za večjo koherentnost in učinkovitost na tem področju na ravni EU ter nacionalni in regionalni ravni. Načrt presega obseg raziskav in razvoja ter inovacije s črko „I“ omenja v naslovu evropskega programa. Izkazalo se je, da je njegova usmeritev k inovacijam in uvajanju varnostnih tehnologij še pomembnejša v trenutnem kontekstu globalnih okoljskih in gospodarskih izzivov.

ESRIF je 23. novembra sprejel glavne ugotovitve in priporočila (za več informacij o ESRIF in njegovem pristopu glej tudi priloženi povzetek končnega poročila ESRIF).

To sporočilo vsebuje **prvoten odziv Komisije na glavne ugotovitve in priporočila ESRIF**.

[1] COM (2007) 511 konč.

## 2. DRUŽBENA RAZSEŽNOST VARNOSTI

ESRIF je pri pristopu k varnostnim raziskavam upravičeno izhajal iz pojmovanja, da je varnost predvsem človeški in družbeni pojav. Ljudje niso samo cilj in žrtve napadov in varnostnih groženj, ampak tudi rešujejo, odločajo in se odzivajo na stanja, ko je varnost ogrožena.

Za obvladovanje teh izzivov morajo vse varnostne rešitve temeljiti na evropskih vrednotah svobode in pravice ter temeljnih etičnih načelih in zakonskih zahtevah, vključenih v vse varnostne dejavnosti na področju raziskav in razvoja ter inovacij. To pomeni:

a) Okrepitev pravne in etične razsežnosti

Varnostni ukrepi niso mogoči brez spoštovanja pravic in svobode posameznikov, zlasti varstva zasebnosti državljanov. Biti morajo zakoniti in sorazmerni, da jih družba sprejme, vedno pa se morajo uporabljati po načelih pravne države. Temeljna etična načela in zahteve varnostnih ukrepov po varstvu podatkov morajo biti temelj za razvoj in izvajanje varnostnih programov. ESRIF se zavzema, da se zahteve po zasebnosti postavijo vzporedno zahtevam po okrepitvi varnosti že od zgodnje faze razmišljanja o novih varnostnih rešitvah. To imenuje „vgrajena zasebnost“.

Takšen pristop, ki ga Komisija pozdravlja, bo imel globoke posledice v celotnem ciklusu raziskav in inovacij.

b) Okrepitev družbene razsežnosti

Nadaljnjo družbeno razsežnost je treba upoštevati s stališča učinkovitosti tehnologij. Brez aktivne udeležbe široke javnosti (in sprejetja z njene strani) ne more biti nobena varnostna tehnologija resnično dolgoročna varnostna rešitev. ESRIF trdi, da pristop na podlagi družbene varnosti pomeni vizijo varnosti, ki se ne osredotoča na preprečevanje in varstvo za vsako ceno, ampak se kaže v zmogljivosti naše družbe, da se spoprime s tveganji, včasih tudi z izgubami, ter si opomore po njih. Takšna „družbena odpornost“ je enako odvisna od svobodne volje obveščenih državljanov kot od kakovosti tehničnih sistemov in zmožnosti podjetij in uprav za neprekinjeno poslovanje.

Za doseganje odpornosti je treba širši javnosti nameniti posebne programe za ozaveščanje o grožnjah, izboljšanje razumevanja uvedenih postopkov za spoprijemanje z izzivi ter nenazadnje za razpravo o sprejemljivosti varnostnih rešitev. Posebne pobude, ki vključujejo medije, so prednostnega pomena. Skladno s poročilom ESRIF so potrebne nadaljnje raziskave o odnosu med novimi tehnologijami ter državljanskimi in človekovimi pravicami.

## 3. IZBOLJŠANJE KONKURENČNOSTI EVROPSKE VARNOSTNE INDUSTRIJE

Varnostna industrija EU, katere ocenjena tržna vrednost je leta 2008 znašala med 26 in 36 milijardami eurov[2], hitro raste in zaposluje visoko usposobljeno delovno silo ter zelo veliko

[2] Varnostna industrija vključuje tradicionalno varnostno industrijo (predvsem dobavo splošnih varnostnih aplikacij, kot je na primer fizični nadzor dostopa), varnosti namenjeno obrambno industrijo (na podlagi uporabe obrambnih tehnologij v varnostnih aplikacijah ali z nabavo in pretvorbo civilnih tehnologij v varnostne aplikacije) ter novosti, tj. predvsem podjetja, ki širijo obstoječe (civilne) tehnologije na varnostne aplikacije, na primer podjetja za IT.

vlaga v raziskave in razvoj. ESRIF priporoča oblikovanje „trdne in neodvisne tehnološke in znanstvene osnove za EU, da se zaščitijo interesi njenih državljanov in njeni industriji omogoči zagotavljanje konkurenčnih izdelkov in storitev“. Priporoča, da EU prevzame vodilno vlogo na varnostnem trgu in podpre pobudo za vodilni trg v varnostnem sektorju.

Zato je treba v ambiciozno industrijsko politiko za varnostni sektor vlagati danes, da bomo lahko jutri imeli koristi od inovacij in rasti:

a) Odpravljanje tržne razdrobljenosti

Varnostna industrija v Evropi mora postati konkurenčnejša in učinkovitejša. Do zdaj je industrija trpela zaradi razdrobljenosti trgov, ki so bili usmerjeni nacionalno ali celo regionalno. Zaradi majhnosti so bili neučinkoviti in slabo stroškovno učinkoviti tako za industrijo kot za končne uporabnike. To je pomembna ovira na poti k interoperabilnosti in povezovanju varnostnih rešitev na nacionalni in evropski ravni. Reševanje problema z oblikovanjem evropskih trgov bo tej industriji omogočilo, da postane konkurenčnejša in privlačnejša na globalni ravni, javna sredstva pa se bodo učinkoviteje porabljala.

(i) Certificiranje, potrjevanje in standardizacija

Na podlagi zahtev končnih uporabnikov in rezultatov raziskav novih tehnologij in rešitev ni treba samo potrjevati, ampak tudi certificirati in po potrebi standardizirati, da lahko postanejo del učinkovitega odziva na varnostne grožnje. Raziskave in razvoj morajo biti povezane z jasno strategijo potrjevanja in javnih naročil, ki upošteva relevantna vprašanja politike in gospodarske interese. To mora spodbujati oblikovanje evropskega varnostnega trga in boljše sodelovanje med zainteresiranimi stranmi na področju varnosti na nacionalni in evropski ravni. ESRIF priporoča, da Komisija oceni uporabnost in učinkovitost „evropske varnostne oznake“.

CEN in ETSI[3] sta že začela s standardizacijo na področju varnosti. CEN se bo najprej ukvarjal s številnimi zadevami, za katere je prejel pooblastila za standardizacijo (zlasti glede varnosti dobavne verige, zaščite kritične infrastrukture ter izdelkov, ki ne dopuščajo zlorab). Ker so standardi lahko učinkovito sredstvo za prenos izsledkov raziskav v inovativne izdelke, je pričakovati, da bo delu v okviru 7. okvirnega programa sledila nadaljnja standardizacija. To delo je treba pospešiti.

Medtem Komisija išče načine za preskušanje rezultatov ustreznih raziskav zaradi oblikovanja prihodnjih mehanizmov certificiranja. Takšni mehanizmi bi morali biti namenjeni certificiranju, da so varnostni izdelki in procesi skladni z ustreznimi standardi.

(ii) Regulativni okvir

ESRIF je poudaril, da bi bilo glede na razdrobljenost varnostnega trga, ki pogosto izhaja iz različne nacionalne zakonodaje, koristno oblikovati usklajen regulativni okvir na posebnih področjih v povezavi z zgodnjim usklajevanjem. Komisija meni, da je kot prvi korak potrebna temeljita analiza obstoječega regulativnega okvira.

---

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

(iii) Interoperabilnost

Skupna uporaba sredstev in informacij utrjuje našo sposobnost odziva na zapletena in čezmejna varnostna vprašanja. Izmenjava informacij med nacionalnimi organi in drugimi evropskimi udeleženci je bistvena za boj proti čezmejnemu kriminalu. Vendar takšno izmenjavo in souporabo informacij danes ovira pomanjkanje tehnične in organizacijske interoperabilnosti. Zato obstaja izrazita potreba po razvoju standardov interoperabilnosti.

b) Krepitev industrijske osnove

Evropska unija potrebuje trdno industrijsko in tehnološko osnovo, da lahko državljanom v EU in drugje zagotavlja moderne varnostne rešitve. Za okrepitev evropske varnostne industrijske in tehnološke osnove je treba obravnavati naslednje zadeve:

(i) Popis varnostne industrijske osnove

Za pridobitev natančne slike o evropski varnostni tehnološki in industrijski osnovi (ESTIB – European Security Technological and Industrial Base) je pomembno popisati te kompetence. S takšnim popisom bo mogoče ugotoviti močne in šibke plati ESTIB ter določiti ustrezne ukrepe za njeno okrepitev. Posebno pozornost bi bilo treba nameniti malim in srednjim podjetjem. Poudariti bi bilo treba tudi sektorje „ključne proizvodnje“ (na primer proizvodnjo električne opreme itd.), ki igra podobno vlogo v proizvodnji kot ključna infrastruktura v infrastrukturnem sektorju.

(ii) Inovacijska politika

Inovacijska politika se osredotoča na prenos znanja v nove izdelke in metode ter hkrati v gospodarsko vrednost in komercialni uspeh[4]. To je še zlasti pomembno za raziskave in razvoj na področju varnosti. Komisija bo zato analizirala, v kolikšni meri je mogoče najbolj inovativne varnostne sektorje vključiti v pobudo za vodilni trg.

Poleg tega so predkomercialna javna naročila koristno orodje za okrepitev javnih naročil inovativnih izdelkov in tehnologij[5]. Komisija bo opravila dodatne analize o možnostih hitrejših predkomercialnih javnih naročil na varnostnem področju. Kar zadeva javna naročila, se Direktiva 2009/81/ES[6] enako uporablja za dobavo obrambne in občutljive opreme. Komisija bo predlagala načine za zagotovitev, da se ta direktiva na varnostnem področju uporablja pregledno in usklajeno.

(iii) Vgrajena varnost

ESRIF priporoča „spodbujanje pristopa *vgrajene varnosti* v vseh na novo razvitih kompleksnih sistemih ali izdelkih, da se varnost zagotovi že v fazi zasnove, kot je bilo pri *vgrajeni zaščiti*“.

---

4 COM(2005) 488 konč.
5 COM(2007) 799 konč.
6 UL L 216 z dne 20.8.2009.

Komisija pozdravlja to priporočilo in bo preučila načine za zagotovitev, da bodo raziskovalne dejavnosti z možnimi varnostnimi učinki po potrebi to upoštevale že v najzgodnejših fazah.

(iv) Sinergije med civilnimi in obrambnimi tehnologijami

Čedalje tesnejša povezanost obrambnih tehnologij na eni strani in varnostnih tehnologij na drugi je zlasti vidna na področju raziskav in razvoja v smislu potencialnega razvoja tehnologij na obeh področjih.

Treba je okrepiti dopolnilne ukrepe in sodelovanje na posebnih področjih, na katerih je mogoče uporabljati tehnologije v civilne in obrambne namene, vključno z nadzorom meja in kibernetsko varnostjo. Na podlagi poziva za nadaljnjo krepitev sinergij med dejavnostmi iz okvirnega programa za raziskave in razvoj ter obrambnim področjem, ki ga je Evropski svet potrdil decembra 2008, je treba zagotoviti sodelovanje z Evropsko obrambno agencijo.

## 4. NALOŽBA V PRIHODNOST

ESRIF je v svojem evropskem programu za varnostne raziskave in inovacije (ESRIA – European Security Research and Innovation Agenda) določil načrt za raziskave in razvoj na področju varnosti za naslednjih 15 let in navedel sistemske zahteve. Treba je razlikovati med ukrepi raziskav in razvoja in ukrepi za zagotavljanje dejanske uvedbe tehnoloških dosežkov iz raziskav in razvoja v novo tehnologijo:

a) Varnostne naloge in prednostne naloge za raziskave in razvoj

ESRIF je v zvezi z raziskavami in razvojem poudaril, da glavne raziskave v podporo varnostnim nalogam, določenim v okviru 7. okvirnega programa, še vedno veljajo za bližnjo prihodnost. Dolgoročno jih je treba ponovno oceniti ter morebiti okrepiti in razširiti.

ESRIF je poudaril, da groženj za evropsko varnost ni mogoče v celoti napovedati, ne glede na to, ali jih povzroča človek ali narava. Zato se morajo raziskave in razvoj na področju varnosti usmeriti h krepitvi odpornosti Evrope na grožnje in njeni sposobnosti, da si uspešno opomore po krizah. To zahteva tudi večjo kohezivnost in trdnost družbenih sistemov in njihovo povezanost s tehnologijami. V tem kontekstu je ESRIF priporočil okrepitev in razširitev raziskav o zaščiti ključne infrastrukture, na primer v zvezi z energetsko varnostjo in varnostjo transportnih omrežij[7].

(i) Razvijajoče se prednostne naloge

Evropski program za varnostne raziskave in inovacije zajema celoten spekter podpore raziskav in razvoja za trenutne varnostne naloge. Razdeljen je v pet sklopov (glej povzetek ESRIF v prilogi).

Komisija priznava pomen, ki ga ESRIF pripisuje celostnemu pristopu v celotnem programu ESRIA. ESRIA se pri sklicevanju tako na razstreliva ali CBRN kot kritično infrastrukturo ali krizno upravljanje bolj kot na dele osredotoča na celoto in

[7] Glej tudi povezano Direktivo Sveta 2008/114/ES.

poudarja pomen omrežij, referenčnih centrov, interoperabilnosti ter rešitev sistema sistemov. ESRIF tako na primer priporoča pripravo „na izpolnjevanje predvidljivih potreb po vseevropskih omrežnih zmogljivostih ter kompleksnih sistemih na področju zgodnjega opozarjanja in pripravljenosti na ukrepanje, povezanih z incidenti, ki jih povzročata narava in človek“.

ESRIF zagovarja inovacije v podporo „celostnemu pristopu“ za upravljanje meja, ki so ga že razvile EU in države članice v schengenskem modelu štiristranskega nadzora dostopa[8], ki je jedro integriranega upravljanja meja. ESRIF poudarja pomen interoperabilnosti in meni, da „morajo raziskave zajemati tehnične vidike interoperabilnosti med razvitimi sistemi ter interoperabilnost na organizacijski ravni ob upoštevanju različnosti čezmejnih kultur. Interoperabilnost je mogoče okrepiti tudi z usklajenimi ali skupnimi operativnimi postopki za razvoj, nabavo in usposabljanje“.

Meni, da so informacijske in komunikacijske tehnologije „bistvenega pomena za evropsko varnost, ker same po sebi pomenijo ključno infrastrukturo ter so pogoj za druge službe in sektorje“, pri tem pa se zlasti sklicuje na potrebo po raziskovanju za povečanje sistemske odpornosti. ESRIF zagovarja raziskave pravnih okvirov v podporo forenzičnim raziskavam in zbiranju dokazov v okolju IKT.

ESRIF je vesolje označil za „bistveno na različnih varnostnih tehnoloških področjih“ ter poudaril pomen GMES in Galilea pri zagotavljanju „široke palete storitev z dodano vrednostjo v podporo varnosti“ ob sklicevanju na potrebo po varstvu pridobitev iz vesoljskih dejavnosti.

Komisija pozdravlja ta celostni pristop k varnostnim raziskavam in inovacijam.

(ii) Prihodnje naloge

Številne varnostne naloge, ki jih je ESRIF analiziral glede na zahtevane zmožnosti in povezane raziskave, se aktivno preučujejo. Mednje med drugim sodijo upravljanje in nadzor meja, zaščita ključne infrastrukture, vključno z IKT, varnostna politika CBRN, ukrepi za okrepitev varnosti razstreliv in detonatorjev ter pregled blaga in potnikov. Ta varnostna področja bodo dodatno opredeljena v prihodnjem stockholmskem akcijskem načrtu.

Varnostni izzivi IKT so na različnih področjih politik in treba jih je obravnavati ustrezno v okviru arhitekture informacijskega sistema za prihodnjo notranjo varnostno strategijo EU.

ESRIF priznava, da njegova pooblastila niso vključevala raziskovalnih tem, ki bodo v prihodnjih letih postale pomembnejše. To velja zlasti za nekatere naloge v zvezi z zunanjo varnostjo. ESRIF je priporočil, da se „zunanji razsežnosti posveti posebna pozornost“, ker „morajo programi za raziskave in inovacije podpirati ohranjanje miru, humanitarne naloge in naloge za krizno upravljanje, vključno s skupnimi pobudami z drugimi regijami in mednarodnimi organizacijami, zlasti glede razvoja globalnih standardov“.

---

[8] Štiri kategorije so: ukrepi v tretjih državah, sodelovanje s sosednjimi državami, upravljanje mejnega nadzora in nadzorni ukrepi v območju prostega gibanja, vključno s povratkom.

Komisija se strinja, da gre za razvijajoča se področja, vendar meni, da je primerno poglobiti razmislek o razširitvi varnostnih raziskovalnih in razvojnih programov na področja, kot so civilna zaščita in preprečevanje konfliktov ter stabilizacija po krizi.

– Civilna zaščita: Civilna zaščita in varnostne raziskave v podporo dejavnostim civilne zaščite bodo najverjetneje postale pomembnejše, nenazadnje zaradi podnebnih sprememb, kot sta navedla visoki predstavnik in Evropska komisija v dokumentu Evropskemu svetu, v katerem sta podnebne spremembe opisala kot „množitelja groženj“[9]. Dokument poziva k povečanju raziskovalnih zmogljivosti EU v smislu povezave med varnostjo in podnebnimi spremembami. Poleg tega je Komisija v sporočilu o „okrepitvi zmogljivosti odzivanja Unije na nesreče“ poudarila potrebo po izboljšanju preprečevanja in ublažitve nesreč, evropske zmogljivosti odzivanja za civilno zaščito in dragocene podpore raziskav.

– Preprečevanje konfliktov in stabilizacija po krizi: Skupnost že ima na voljo operativno financiranje prek instrumenta za stabilnost[10]. Njegov namen je vzpostavitev ali ponovna vzpostavitev razmer, bistvenih za pravilno izvajanje razvojnih politik Komisije v primeru kriz ali nastajanja kriz, ter pomoč pri razvoju zmogljivosti za obravnavanje posebnih globalnih in medregionalnih groženj kot tudi zagotavljanje pripravljenosti pred krizo in po njej. Vendar na ravni Skupnosti primanjkuje sredstev za raziskave v podporo tem dejavnostim.

b) Ukrepi poleg raziskav in razvoja

(i) Vključitev končnih uporabnikov

ESRIF je ob priporočilu za „*tesno posvetovanje v Evropi* med zainteresiranimi stranmi, ki zagotavljajo ponudbo in povpraševanje ter predstavljajo končne uporabnike, med načrtovanjem, izvrševanjem in pregledom varnostne raziskovalne politike“ ugotovil, da morajo vlade in končni uporabniki sprejeti „ponovno organizacijsko uskladitev za oblikovanje varnostnih inovacij in odziv nanje“.

Komisija se strinja, da si morajo javni in zasebni končni uporabniki na področju varnosti pogosto več prizadevati za okrepitev baze znanja o varnostni tehnologiji in bodočih analitičnih zmogljivostih, da bodo lahko v celoti izkoristili priložnost za zagotovitev ustreznosti prihodnjih rešitev dejanskim potrebam, na primer z modeli demonstracije.

(ii) Prihodnji programi za razširjanje inovativnih rešitev

Komisija je že omenila koristnost naložb v operativne vidike varnosti, zlasti za številna področja, na katerih nacionalni in mednarodni organi uporabljajo tehnološke rešitve[11]. ESRIF meni, da je uspeh na globalnem trgu zelo odvisen od referenc, pridobljenih z javnimi naročili na trgu EU, ter priporoča izkoriščanje predkomercialnih javnih naročil za inovativne rešitve.

---

9 Glej 7249/08, 3.3.2008. Glej tudi sporočilo Komisije o „okrepitvi zmogljivosti odzivanja Unije na nesreče“ (COM(2008) 130 konč.).

10 Uredba (ES) št. 1717/2006, UL L 327, str. 1, 24.11.2006.

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

ESRIF podpira razvoj modela na podlagi strateškega in koordiniranega pristopa k vseevropskemu sodelovanju. Vseevropska omrežja omenja kot zgled, ki naj bo referenca za sistemsko integracijo na ravni EU v varnostno območje. Tako kot za TEN bo financiranje zagotovljeno za dopolnitev nacionalnih sredstev za zaščito evropske kritične infrastrukture. Ker je za popoln odziv na pričakovanja uporabnikov treba izkoristiti razpoložljiva sredstva za raziskave in tehnološki razvoj, je ESRIF omenil, da bi v podporo procesu lahko ustanovili notranji varnostni sklad.

(iii) Izobraževanje in usposabljanje

ESRIF je poudaril pomen povezovanja izobraževanja in usposabljanja na področju raziskav ter odgovornost zanj pripisal vsem zainteresiranim stranem: varnostnim uradnikom, oblikovalcem politike, organom pregona, civilni družbi, industriji, raziskovalnim organizacijam, akademski sferi in medijem. Podpira nove programe ozaveščanja, namenjene širši javnosti, za ozaveščanje o grožnjah, tveganjih in ranljivosti ter za izboljšanje razumevanja politik in tehnoloških rešitev, potrebnih za varnost.

## 5. IZVAJANJE EVROPSKEGA PROGRAMA ZA VARNOSTNE RAZISKAVE IN INOVACIJE

Priporočila ESRIF o vodenju obravnavajo načine za zagotavljanje posodobitve ESRIA in intenzivnejšo vključitev vseh ustreznih zainteresiranih strani. ESRIF priporoča, da *je treba za uravnoteženo in dosledno izvajanje ESRIA vzpostaviti pregleden mehanizem, ki bo vključeval vse zainteresirane strani.*

Ker so varnostne raziskave usmerjene k uporabnikom in temeljijo na zmogljivosti, ESRIF meni, da je treba vzpostaviti ustrezno povezanost in mehanizme izmenjave med končnimi uporabniki ter raziskovalnimi dejavnostmi in industrijo.

## 6. SKLEP

To sporočilo je prvotni odziv Komisije na končno poročilo ESRIF. Komisija meni, da so rezultati dela ESRIF pomembni, in pozdravlja njegovo strateško usmeritev. Preučila je njegova priporočila in poudarja naslednje teme, ki bi jih naslednja Komisija morda želela nadalje analizirati:

- vloga Agencije Evropske unije za temeljne pravice[12][13], da opravi raziskave o povezavi med varnostjo in zasebnim življenjem ter varstvom podatkov;

- potreba po okrepitvi „etičnega preverjanja“ projektov, ki se pregledujejo v okviru teme varnost iz 7. okvirnega programa, ter omogočanje dostopnosti rezultatov tekočih projektov raziskav in razvoja na področju varnosti najširši javnosti;

- družbena razsežnost kot neločljiv pričakovani učinek vseh svojih razpisov za zbiranje predlogov v okviru teme varnost iz 7. okvirnega programa;

---

12 Sklep Sveta št. 2008/203/ES, UL L 63, 7.3.2008.

13 Uredba št. 168/2007, UL L 53, 22.2.2007.

- možnost vključitve najbolj inovativnih varnostnih sektorjev v pobudo za vodilni trg;
- načini za pospešitev predkomercialnih javnih naročil na varnostnem področju;
- načini za pospešitev certificiranja, potrjevanja in po potrebi standardizacije na področju varnosti, zlasti glede uporabnosti in učinkovitosti „evropske varnostne oznake“;
- načini za najboljši odziv na predvidljive nove varnostne in prednostne naloge, bodisi v okviru trenutnega 7. okvirnega programa bodisi pri pripravi prihodnjega okvirnega programa;
- načini za boljšo povezanost evropskih varnostnih raziskav in razvoja z bolj operativnimi vidiki varnosti na ravni EU in držav članic;
- vzpostavitev stalne delovne strukture za izvajanje priporočil ESRIF;
- možnost oblikovanja foruma za okrepitev konkurenčnosti varnostne industrije, dejavne na področju raziskav in inovacij, kot je skupina na visoki ravni, ob sodelovanju vseh zainteresiranih strani javnega in zasebnega sektorja ter civilne družbe.

## 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.