H4 33074 PE European Security Research and Innovation Agenda

COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le 21.12.2009
COM(2009)691 final

COMMUNICATION DE LA COMMISSION

«Agenda européen de la recherche et de l'innovation en matière de sécurité - Position initiale de la Commission sur les principales constatations et recommandations du forum ESRIF»

EN

COMMUNICATION DE LA COMMISSION

«Agenda européen de la recherche et de l'innovation en matière de sécurité - Position initiale de la Commission sur les principales constatations et recommandations du forum ESRIF»

1. INTRODUCTION

L'un des principaux objectifs de l'Union européenne est de préserver et de développer les valeurs européennes de justice, de liberté et de sécurité tout en relevant les défis toujours plus complexes en matière de sécurité.

La lutte contre le terrorisme et le crime organisé, la protection des frontières extérieures de l'Europe et la gestion civile des crises ont pris de l'importance dans notre vie quotidienne. Le changement climatique, s'il n'est pas correctement traité, pourrait avoir des effets déstabilisateurs à l'échelle mondiale. Dans le même temps, la sécurité intérieure et la sécurité extérieure sont de plus en plus inséparables. Pour les assurer, des technologies modernes sont nécessaires.

Puisque les technologies de sécurité sont de plus en plus présentes dans les sociétés modernes et suscitent parfois des préoccupations de la part des citoyens, il est essentiel de garantir le contrôle éthique et la transparence des projets de recherche et de développement en matière de sécurité. Notre sécurité doit s'appuyer sur nos valeurs européennes et, inversement, des solutions de sécurité sont nécessaires pour protéger nos valeurs sociétales.

Il faudra, pour répondre à ces préoccupations dans les années qui viennent, une meilleure compréhension de l'interaction entre les facteurs humains et naturels qui peuvent causer des risques de sécurité; par ailleurs cette meilleure compréhension est également essentielle pour concevoir des réponses efficaces, parallèlement au recours à la technologie moderne et aux solutions innovantes.

La Commission a estimé qu'afin de trouver les réponses les plus efficaces à ces défis, il était indispensable de réunir des représentants de l'industrie, des utilisateurs finals publics et privés, des établissements de recherche et des universités ainsi que d'organisations non gouvernementales et d'institutions de l'UE. Elle a donc proposé, en 2007, d'instaurer conjointement avec les États membres un «Forum européen de la recherche et de l'innovation en matière de sécurité» - ESRIF[1].

L'ESRIF a été chargé d'élaborer un «agenda européen de la recherche et de l'innovation en matière de sécurité»: une feuille de route stratégique pour la recherche et l'innovation en matière de sécurité visant à apporter une cohérence et une efficacité plus grandes à ce domaine qui englobe les niveaux européen, national et régional. Au-delà de la recherche et du développement, il vise à inscrire le «I» d'Innovation dans l'agenda européen. Son orientation vers l'innovation et l'application des technologies de sécurité se révèle beaucoup plus importante dans le contexte des défis environnementaux et économiques au niveau mondial.

[1] COM (2007) 511 Final

Le 23 novembre, l'ESRIF a adopté ses principales conclusions et recommandations (pour plus d'information sur l'ESRIF et son approche, voir également le résumé analytique ci-joint du rapport final de l'ESRIF)

Cette communication présente **la réaction initiale de la Commission aux principales conclusions et recommandations de l'ESRIF.**

2. DIMENSION SOCIETALE DE LA SECURITE

À juste titre, l'ESRIF a fondé son approche de la recherche en matière de sécurité sur la perspective que la sécurité est avant tout humaine et sociétale. Elle concerne non seulement les personnes qui sont les cibles et les victimes d'attaques et de menaces, mais aussi les sauveteurs, les décideurs et tous ceux qui sont confrontés à des situations d'insécurité.

Pour relever ces défis, toutes les solutions en matière de sécurité doivent être fondées sur les valeurs européennes de liberté et de justice, sur les principes éthiques fondamentaux, ainsi que sur les exigences légales qui sont au cœur de toutes les activités de recherche et de développement et d'innovation en matière de sécurité. Cela signifie:

a) Renforcement dans la dimension légale et éthique

Il ne peut exister des mesures de sécurité qui ne prennent en considération le respect des droits et libertés des personnes, plus particulièrement en ce qui concerne la protection de la vie privée. Les mesures de sécurité doivent être légitimes et proportionnées afin d'être acceptées par l'opinion et doivent toujours être appliquées conformément à l'état de droit. Les principes éthiques fondamentaux et les exigences relatives à la protection des données doivent être la base de l'élaboration et de la mise en œuvre des programmes de sécurité. L'ESRIF préconise que les exigences relatives à la vie privée soient prises en considération conjointement avec les exigences en matière de renforcement de la sécurité dès le stade le plus précoce, lorsque de nouvelles solutions en matière de sécurité sont envisagées. C'est ce qu'il appelle «Privacy by design» (prise en compte de la vie privée dès la conception).

Cette approche, qui est accueillie favorablement par la Commission, aura de profondes conséquences sur l'ensemble du cycle de recherche et d'innovation.

b) Renforcement de la dimension sociétale

Une dimension sociétale supplémentaire doit être prise en considération du point de vue de l'efficacité des technologies. Aucune technologie de sécurité ne peut effectivement être une solution en matière de sécurité à long terme sans la participation active (et l'acceptation) du grand public. En effet, l'ESRIF fait valoir qu'une approche sociétale de la sécurité implique une vision de la sécurité qui n'est pas axée sur la prévention et la protection à tout prix, mais réside plutôt dans la capacité de nos sociétés de faire face aux risques, et parfois aux pertes, et de s'en rétablir. Cette «résilience sociétale» dépend autant de la libre volonté de citoyens informés que de la qualité des systèmes techniques et de la capacité des entreprises et des administrations de poursuivre leurs activités.

Pour obtenir la résilience, il faut des programmes spécifiques s'adressant à un large public et visant à sensibiliser aux menaces, à améliorer la compréhension des processus mis en place pour relever les défis ainsi qu'à débattre de l'acceptabilité des solutions en matière de sécurité. Des initiatives spécifiques impliquant les médias ont la priorité. Comme l'indique le

rapport de l'ESRIF, il convient de poursuivre les recherches sur la relation entre les nouvelles technologies, les droits civils et les droits de l'homme.

3. AMELIORER LA COMPETITIVITE DE L'INDUSTRIE EUROPEENNE DE LA SECURITE

L'industrie de la sécurité de l'UE, qui représentait un marché de 26 à 36 milliards d'euros[2] en 2008, est en croissance rapide, emploie une main-d'œuvre hautement qualifiée et présente une forte composante de R&D. L'ESRIF recommande la recherche d'une «base technologique et scientifique forte et indépendante pour que l'UE soit en mesure de protéger les intérêts de ses citoyens et que son industrie puisse fournir des produits et services d'une manière compétitive». Il recommande que l'UE vise la première position sur le marché de la sécurité et soutient l'idée d'une initiative «marchés porteurs» dans le secteur de la sécurité.

Cela nécessite cependant d'investir maintenant dans une politique industrielle ambitieuse dans le secteur de la sécurité, afin de récolter demain l'innovation et la croissance:

a) Surmonter la fragmentation du marché

L'industrie de la sécurité en Europe doit devenir plus compétitive et efficace. Elle a souffert jusqu'à présent de la fragmentation des marchés, qui tendent à avoir une dimension nationale ou même régionale. Leur petite taille les rend inefficaces et aboutit à un mauvais rapport coût-efficacité tant pour l'industrie que pour les utilisateurs finals. C'est un obstacle important pour l'interopérabilité et l'intégration des solutions en matière de sécurité au niveau national et européen. La résolution de ce problème, par la création de marchés de dimension européenne, rendra cette industrie plus compétitive et attractive au niveau mondial et entraînera une plus grande efficacité des dépenses publiques.

i) Certification, validation et normalisation

Sur la base des exigences des utilisateurs finals et des résultats de la recherche, de nouvelles technologies et solutions doivent non seulement être validées, mais aussi certifiées et, le cas échéant, normalisées, de manière à pouvoir faire partie intégrante d'une réponse efficace aux menaces pesant sur la sécurité. Les activités de R&D devraient être associées à une stratégie claire de validation et de passation des marchés, prenant en considération les problèmes politiques pertinents ainsi que les intérêts économiques, ce qui devrait promouvoir la création d'un marché européen de la sécurité et une meilleure coopération entre les partenaires de la sécurité au niveau national et européen. L'ESRIF recommande que la Commission évalue l'applicabilité et l'efficacité d'un «label de sécurité européen».

---

[2] L'industrie de la sécurité recouvre l'industrie de la sécurité traditionnelle (fondée sur la fourniture des applications en matière de sécurité générale telles que, par exemple, le contrôle de l'accès physique), l'industrie de défense axée sur la sécurité (fondée sur l'utilisation de technologies de défense dans les applications en matière de sécurité ou l'acquisition de technologies civiles et leur conversion aux applications en matière de sécurité) ainsi que les nouveaux entrants, principalement des sociétés qui étendent leur technologie existante (civile) à des applications en matière de sécurité, telles que, par exemple, les sociétés informatiques.

Le CEN et l'ETSI[3] ont commencé à travailler sur une normalisation dans le domaine de la sécurité. Le CEN se concentre d'abord sur un certain nombre de problèmes pour lesquels il a reçu des mandats de normalisation (notamment en ce qui concerne la sécurité de la chaîne d'approvisionnement, la protection des infrastructures critiques et la protection des produits contre la criminalité). Étant donné que les normes peuvent être le moyen efficace de traduire les résultats de la recherche en produits innovants, les travaux accomplis dans le cadre du 7e PC devraient aboutir à une normalisation plus poussée. Ces travaux doivent être accélérés.

Pendant ce temps, la Commission examine de quelle manière les résultats des actions de recherche pourraient être éprouvés afin d'élaborer de nouveaux mécanismes de certification. Ces derniers devraient avoir pour objectif de certifier que les produits et les processus en matière de sécurité sont conformes aux normes applicables.

ii) Cadre réglementaire

L'ESRIF a souligné qu'étant donné la fragmentation du marché de la sécurité, fréquemment due aux différences entre les législations nationales, il serait recommandé d'instaurer un cadre réglementaire harmonisé dans des domaines spécifiques combinés avec une coordination en amont. La Commission considère qu'en tant que première étape, une analyse approfondie du cadre réglementaire actuel est nécessaire.

iii) Interopérabilité

Le partage des ressources et des informations renforce notre capacité de traiter des problèmes de sécurité complexes et transfrontaliers. L'échange d'informations entre les autorités nationales et les autres acteurs européens est essentiel pour lutter contre la criminalité transfrontalière. Toutefois, le manque d'interopérabilité technique et organisationnelle entrave l'échange et le partage d'informations. Il est donc urgent de mettre au point des normes d'interopérabilité.

b) Renforcement de la base industrielle

L'Union européenne a besoin d'une base industrielle et technologique forte pour offrir des solutions de sécurité modernes aux citoyens dans l'UE et dans le reste du monde. Les problèmes suivants doivent être réglés afin de renforcer la base industrielle et technologique de la sécurité européenne:

i) Cartographie de la base industrielle de la sécurité

Afin d'obtenir une image précise de la base technologique et industrielle de la sécurité européenne (ESTIB), il est important de cartographier ces compétences. Cette cartographie permettra d'identifier les points forts et faibles de l'ESTIB et permettra de définir des mesures appropriées pour la renforcer. Il convient de prêter une attention particulière aux PME. Les secteurs de «fabrication critique» (tels que par exemple la fabrication d'équipements électriques, etc.) – qui jouent par rapport à

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

la fabrication un rôle similaire à celui des infrastructures critiques par rapport aux infrastructures – devraient également être mis en relief.

ii) Politique de l'innovation

La politique de l'innovation vise à transformer la connaissance en nouveaux produits et méthodes ainsi qu'en valeur économique et en succès commercial[4]. Cela est particulièrement pertinent pour la R&D en matière de sécurité. La Commission analysera donc la manière dont les secteurs de sécurité les plus innovants devraient être intégrés dans l'initiative «marchés porteurs».

En outre, les achats publics avant commercialisation sont un instrument utile pour encourager les achats publics de produits et technologies innovants[5]. La Commission poursuivra son analyse de la manière d'accélérer les achats publics avant commercialisation dans le domaine de la sécurité. En ce qui concerne les marchés publics, la directive 2009/81/CE[6] s'applique également à la fourniture d'équipements de défense et d'équipements sensibles. La Commission proposera des solutions pour veiller à ce que cette directive soit appliquée de manière transparente et harmonisée dans le domaine de la sécurité.

iii) Sécurité dès le stade de la conception

L'ESRIF recommande «la promotion d'une approche de la *sécurité dès le stade de la conception* pour tout système ou produit complexe récemment élaboré, garantissant que la sécurité est traitée au moment de la conception, comme dans le cas de la *sûreté dès le stade de la conception*».

La Commission approuve cette recommandation et examinera les moyens de garantir, le cas échéant, que toutes les activités de recherche ayant des effets en termes de sécurité soient prises en considération dès les stades les plus précoces.

iv) Synergies entre technologies civiles et de défense

La nature évolutive des relations entre les technologies de la défense d'une part et les technologies de la sécurité de l'autre est particulièrement notable dans le domaine de la R&D, avec des technologies présentant des évolutions potentielles dans les deux domaines.

Il est nécessaire de renforcer la complémentarité et la coopération dans des domaines spécifiques dans lesquels les technologies peuvent avoir des applications en matière civile et de défense, y compris dans les domaines du contrôle aux frontières et de la cybersécurité. Sur la base d'un appel approuvé par le Conseil européen de décembre 2008 à renforcer encore les synergies entre les activités menées dans le cadre du programme de R&D et le domaine de la défense, il convient d'assurer une coopération étroite avec l'agence européenne de défense (AED).

---

4 COM(2005) 488 final.
5 COM (2007) 799 final.
6 JO L 216 du 20.8.2009

4. INVESTIR DANS L'AVENIR

L'ESRIF a présenté, dans son agenda européen de la recherche et de l'innovation en matière de sécurité (ESRIA), une feuille de route de la R&D en matière de sécurité pour les quinze prochaines années, incluant également des exigences systémiques. Il convient d'établir une distinction entre les mesures de R&D et les mesures visant à garantir que tous les progrès technologiques accomplis par la R&D aboutissent au déploiement actuel de cette nouvelle technologie:

a) les missions et priorités de la sécurité en matière de R&D

En termes de R&D, l'ESRIF a souligné que la recherche principale soutenant les missions de sécurité définies par le 7e PC demeure valide pour l'avenir immédiat. À plus long terme, ces missions devront être réévaluées et, éventuellement, renforcées et amplifiées.

L'ESRIF a souligné qu'il n'est pas possible de prévenir totalement les menaces pour la sécurité de l'Europe, qu'elles soient d'origine naturelle ou humaine. C'est pourquoi, la R&D en matière de sécurité doit se concentrer sur le renforcement de la résilience de l'Europe aux menaces et sur sa capacité de surmonter les crises. Cela inclut également le renforcement de la cohérence et de la solidité des systèmes sociétaux et de leur interface avec les technologies. Dans ce contexte, l'ESRIF a recommandé que la recherche sur la protection des infrastructures critiques soit renforcée et amplifiée, en ce qui concerne par exemple la recherche de la sécurité énergétique et la sécurité du réseau de transport[7].

i) des priorités en développement

L'agenda européen de la recherche et de l'innovation en matière de sécurité (ESRIA) couvre le spectre complet du soutien en matière de R&D aux missions de sécurité actuelles. Il est regroupé en cinq volets (voir le résumé analytique de l'ESRIF en annexe).

La Commission souligne l'accent mis par l'ESRIF sur une approche intégrée dans l'ESRIA tout entier. Qu'il s'agisse des explosifs ou des menaces CBRN, des infrastructures critiques ou de la gestion de crise, l'ESRIA se concentre sur la totalité plutôt que sur les parties, en soulignant l'importance des réseaux, des centres de référence, de l'interopérabilité et des solutions «système de systèmes». En effet, l'ESRIF recommande, par exemple, de se préparer à «satisfaire les besoins prévisibles de capacités en réseau au niveau européen et de systèmes complexes d'alerte précoce et de réaction rapide aux accidents d'origine naturelle et humaine».

Il préconise l'innovation soutenant une «approche holistique» de la gestion des frontières qui, en fait, a été élaborée par l'UE et les États membres dans le modèle de Schengen de contrôle d'accès à quatre niveaux[8], qui est le fondement de la gestion intégrée des frontières. L'ESRIF souligne l'importance de l'interopérabilité, du fait que «la recherche doit couvrir les aspects d'interopérabilité technique entre les systèmes déployés ainsi que l'interopérabilité au niveau organisationnel, compte tenu de la diversité des cultures transfrontalières. L'interopérabilité peut également être

---

7 Voir également à ce sujet la directive 2008/114/CE du Conseil.

8 Les quatre niveaux sont: mesures dans les pays tiers, coopération avec les pays voisins, gestion du contrôle aux frontières et mesures de contrôle dans l'espace de libre-circulation, y compris le retour.

renforcée par des procédures opérationnelles harmonisées ou communes pour le développement, l'acquisition et la formation».

L'ESRIF estime que les technologies de l'information et des communications sont «d'une importance cruciale pour la sécurité européenne, puisqu'il s'agit d'infrastructures critiques en elles-mêmes, et elles sont aussi des catalyseurs dont dépendent d'autres services et secteurs», en se référant notamment aux besoins de recherche pour accroître la résilience systémique. L'ESRIF préconise la recherche sur les cadres juridiques afin de soutenir la criminalistique et la collecte de preuves dans l'environnement TIC.

L'ESRIF a qualifié le rôle de l'espace de «vital dans divers domaines liés à la sécurité» et a souligné l'importance du GMES et de Galileo pour fournir «une large gamme de services à valeur ajoutée pour soutenir la sécurité» en se référant aux besoins de protéger les moyens spatiaux.

La Commission approuve cette approche globale de la recherche et de l'innovation en matière de sécurité.

ii) missions futures

Plusieurs des missions de sécurité que l'ESRIF a analysées afin d'en déterminer les besoins en matière de capacité et d'efforts de recherche connexes sont actuellement à l'étude. C'est entre autres le cas de la gestion et du contrôle des frontières, de la protection des infrastructures critiques (y compris les TIC), de la politique de sécurité à l'égard des menaces chimiques, biologiques, radiologiques et nucléaires (CBRN), des mesures destinées à améliorer la sécurité des explosifs et des détonateurs et des mesures d'inspection et de filtrage des marchandises et des voyageurs. Ces domaines de sécurité seront définis de manière plus détaillée dans le futur plan d'action de Stockholm.

Les enjeux que présentent les TIC en matière de sécurité touchent à divers domaines politiques et doivent être traités en conséquence dans le cadre de l'architecture du système d'information qui soutiendra la future stratégie de sécurité intérieure de l'UE.

L'ESRIF a reconnu que son mandat ne couvrait pas certains domaines de recherche voués à prendre de l'ampleur dans les prochaines années, en particulier à l'égard de certaines missions de sécurité extérieure. L'ESRIF a recommandé d'«accorder une haute priorité à la dimension extérieure de la sécurité» compte tenu du fait que «les programmes en matière de recherche et d'innovation doivent soutenir le maintien de la paix, les actions humanitaires et les activités de gestion de la crise, y compris les initiatives communes menées avec d'autres régions et d'autres organisations internationales, notamment en ce qui concerne le développement de normes mondiales».

La Commission considère que, bien que ces domaines soient effectivement en pleine évolution, il convient d'approfondir la réflexion au sujet de l'extension des programmes de recherche et de développement en matière de sécurité à des domaines tels que la protection civile, la prévention des conflits et la stabilisation au lendemain de la crise.

– Protection civile: la protection civile et par conséquent la recherche en matière de sécurité pour étayer les activités de protection civile sont susceptibles de prendre de l'importance, a fortiori dans le contexte du changement climatique, comme l'indique un rapport établi conjointement par le Haut Représentant et la Commission européenne à l'attention du Conseil européen, dans lequel le changement climatique est qualifié de «multiplicateur de menace»[9]. Ce document appelle à renforcer les capacités de l'UE en matière de recherche du point de vue du lien entre sécurité et changement climatique. De plus, dans sa communication intitulée «Renforcer la capacité de réaction de l'Union européenne en cas de catastrophes», la Commission a mis l'accent sur la nécessité d'améliorer la prévention et l'atténuation des catastrophes, sur la capacité de réaction européenne en matière de protection civile et sur l'aide précieuse que peut apporter la recherche.

– Prévention des conflits et stabilisation d'après-crise: la Communauté a déjà mis en place un financement opérationnel par l'intermédiaire de l'instrument de stabilité[10]. Cet instrument vise à établir ou restaurer les conditions essentielles pour permettre la mise en œuvre effective des politiques de développement de la Communauté en cas de crise ou de crise émergente, à contribuer à créer les capacités afin de faire face aux menaces mondiales et transrégionales spécifiques qui ont un effet déstabilisateur et à assurer la préparation pour aborder les situations d'avant-crise et d'après-crise. Toutefois, au niveau communautaire, la recherche manque de fonds pour soutenir ces activités.

b) Au-delà de la recherche et du développement

i) Implication des utilisateurs finals

Tout en recommandant une «*consultation approfondie au niveau européen* avec des représentants de l'offre, de la demande et des acteurs finals lors de la planification, de l'exécution et du cycle d'examen de la politique de recherche en matière de sécurité», l'ESRIF a constaté le besoin pour les gouvernements et les utilisateurs finals d'entreprendre «un réalignement organisationnel afin d'orienter l'innovation en matière de sécurité et d'y répondre».

La Commission convient qu'il faut souvent que les utilisateurs finals de la sécurité, tant publique que privée, fassent un effort supplémentaire pour renforcer la base de leurs connaissances en matière de sécurité et leurs capacités d'analyse prospective, pour être en mesure de profiter pleinement de l'occasion de s'assurer que les solutions futures seront adaptées à leurs besoins réels, au moyen, par exemple, des modèles de démonstration.

ii) Futurs programmes de diffusion de solutions innovantes

La Commission a déjà indiqué l'utilité d'investir dans les aspects opérationnels de la sécurité, notamment dans un certain nombre de domaines dans lesquels les autorités

---

9 Voir document 7249/08 du 3.3.2008. Voir aussi la communication de la Commission intitulée «Renforcer la capacité de réaction de l'Union européenne en cas de catastrophes» (COM(2008) 130 final).

10 Règlement (CE) n° 1717/2006, JO L 327 du 24.11.2006, p. 1.

nationales et internationales utilisent des solutions technologiques[11]. L'ESRIF considère que le succès sur le marché mondial dépend largement des références de marchés publics de l'UE et recommande que les achats publics de solutions innovantes avant la commercialisation soient exploités.

L'ESRIF soutient l'élaboration d'un modèle fondé sur une approche stratégique et coordonnée de la coopération transeuropéenne. Il se réfère aux réseaux transeuropéens en tant qu'exemple qui devrait servir de référence à l'intégration systémique au niveau de l'UE dans le domaine de la sécurité. Comme dans le cas de ces réseaux transeuropéens, un financement serait accordé pour compléter les fonds nationaux afin de garantir la sécurité des infrastructures critiques européennes. Étant donné que les ressources disponibles pour la recherche et le développement technologique doivent être pleinement exploitées pour répondre entièrement aux attentes des utilisateurs, l'ESRIF remarque que ce processus peut être soutenu par la création d'un fond de sécurité interne.

iii) Éducation et formation

L'ESRIF souligne l'importance de l'association de l'enseignement et de la formation dans le domaine de la recherche et estime qu'elle relève de responsabilités de toutes les parties prenantes: responsables de la sécurité, décideurs politiques, forces de police, société civile, industrie, organisations de recherche, universités et médias. Il préconise de nouveaux programmes de sensibilisation aux menaces, risques et vulnérabilités s'adressant au grand public et l'amélioration de sa connaissance des politiques et des solutions technologiques requises en matière de sécurité.

5. MISE EN ŒUVRE DE L'AGENDA EUROPEEN DE LA RECHERCHE ET DE L'INNOVATION EN MATIERE DE SECURITE

Les recommandations de l'ESRIF relatives à la gouvernance examinent comment maintenir à jour l'ESRIA et impliquer plus étroitement toutes les parties prenantes. L'ESRIF préconise qu'un «*mécanisme transparent impliquant tous les partenaires soit créé afin d'appliquer l'ESRIA de manière équilibrée et rigoureuse*».

Étant donné que la recherche en matière de sécurité est orientée vers les utilisateurs et axée sur la capacité, l'ESRIF remarque qu'il existe un besoin d'interfaces adéquates et de mécanismes d'échange entre la communauté des utilisateurs finals et celles de la recherche et de l'industrie.

6. CONCLUSION

Le présent document constitue un avis préliminaire de la Commission sur le rapport final de l'ESRIF. La Commission considère que les résultats obtenus par l'ESRIF sont importants et salue l'orientation stratégique de son travail. Elle prend acte de ses recommandations et souligne les aspects suivants, au cas où la prochaine Commission souhaiterait les approfondir:

[11] COM(2008) 68 final; COM(2008) 130 final, COM (2009) 262 Final.

- le rôle de l'Agence des droits fondamentaux de l'Union européenne[12][13], qui consiste à entreprendre des recherches sur le rapport entre sécurité, vie privée et protection des données;

- la nécessité de renforcer le «contrôle éthique» des projets révisés dans le cadre du thème «sécurité» du 7e PC et de permettre au public le plus large possible d'accéder aux résultats des projets en cours dans le domaine de la R&D;

- la dimension sociétale en tant que résultat escompté inhérent à tous les appels de propositions relatifs au thème «sécurité» du 7e PC;

- la possibilité de faire participer les secteurs les plus innovants en matière de sécurité à l'initiative «marchés porteurs»;

- la façon d'accélérer les achats publics avant commercialisation dans le domaine de la sécurité;

- les solutions pour accélérer les activités de certification, de validation et, le cas échéant, de normalisation dans le domaine de la sécurité, notamment en ce qui concerne l'applicabilité et l'efficacité d'un «label de sécurité européen»;

- la façon d'aborder au mieux les nouvelles missions et priorités prévisibles en matière de sécurité, que ce soit dans le cadre de l'actuel 7e PC ou de la préparation du futur programme-cadre;

- la façon d'établir un lien plus étroit, au niveau de l'Union et des États membres, entre la recherche et le développement liés à la sécurité dans l'Union européenne et les aspects plus opérationnels liés à la sécurité;

- la création d'une structure de travail permanente pour mettre en œuvre les recommandations de l'ESRIF;

- la possibilité de créer un espace de discussion afin de renforcer la compétitivité de l'industrie de la sécurité active dans le domaine de la recherche et de l'innovation, par exemple sous la forme d'un groupe de haut niveau auquel participent toutes les parties prenantes des secteurs public et privé et de la société civile.

---

12 Décision du Conseil n° 2008/203/CE, JO L 63 du 7.3.2008.

13 Règlement n° 168/2007, JO L 53 du 22.2.2007.

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.