



**APPEL A PROJETS 2006**  
**CONCEPTS SYSTEMES ET OUTILS**  
**POUR LA SECURITE GLOBALE**

**Date de publication : 7 avril 2006**

**Date limite de dépôt des dossiers de candidature : 14 Juin 2006 à 12H**

**POUR TOUT RENSEIGNEMENT :**

**les personnes à contacter à l'UTT sont les suivantes :**

E. Châtelet – ec.csosg@utt.fr – Tél : 0325715634  
Ph. Cornu – phc.csosg@utt.fr – Tél : 0325715689

**RESPONSABLE PROGRAMME SECURITE ANR:**

francois.murgadella@agencerecherche.fr

## 1- CONTEXTE

Assurer la sécurité des biens et des personnes dans un espace de liberté et de justice, tel est l'objectif de la stratégie européenne de sécurité adoptée par le Conseil Européen en 2003 et réaffirmée en 2004, suite aux attentats de Madrid.

Le rapport d'un Groupe de Personnalités<sup>1</sup>, mandaté par la Commission Européenne, soulignait la nécessité de financer la recherche sur un très large champ de missions de sécurité, très proche du concept de sécurité globale.

La sécurité globale peut être définie comme la capacité d'assurer à une collectivité donnée et à ses membres, un niveau suffisant de prévention et de protection contre les risques et les menaces de toutes natures et de tous impacts, d'où qu'ils viennent, dans des conditions qui favorisent le développement sans rupture de la vie et des activités collectives et individuelles<sup>2</sup>. Cette définition recouvre de fait les différentes composantes suivantes : sécurité économique, sécurité sanitaire, sécurité informatique et numérique (données, réseaux,...), sécurité du territoire, aérienne et maritime, sécurité civile, lutte contre le terrorisme, la criminalité et la fraude...

Cette approche générale, qui se caractérise par un traitement d'ensemble de la sécurité, systémique et transversal, des causes comme des effets, est celle retenue par la Commission Européenne dans son appel préparatoire sur la recherche en sécurité (PASR<sup>3</sup>). Cette action a pour objectif de préparer le volet sécurité du prochain programme cadre de recherche de l'U.E. (7<sup>ème</sup> PCRD, 2007-2013). Au travers des travaux déjà lancés depuis 2004 et des groupes de réflexions européens réunissant acteurs publics et privés<sup>4</sup>, l'Europe a défini quatre grandes missions de sécurité : la lutte contre le terrorisme et la grande criminalité - la sécurité des infrastructures, des sites et des réseaux - la sécurité des frontières (terrestres et maritimes) - la gestion de crise, intervention et réparation.

Du point de vue national, une coordination interministérielle est en place depuis janvier 2005. Elle a apporté son plein soutien à l'initiative européenne d'un programme sur la sécurité mais a également proposé une typologie de la sécurité (cf. annexe), recensé les besoins étatiques et entamé un dialogue avec les acteurs nationaux de la recherche académique et industrielle en sécurité<sup>5</sup>.

Il apparaît dorénavant nécessaire de lancer un appel à projets de recherche dans un contexte national, en cohérence avec la démarche européenne

Les projets attendus dans le cadre du présent appel à projet 2006, sont des projets de type « recherche industrielle » au sens de la définition de l'Union Européenne<sup>6</sup>.

<sup>1</sup> Research for a secure Europe : report of "Group Of Personalities" (GOP) in the field of security research, 2004, <http://europa.eu.int/comm/research/security>.

<sup>2</sup> Définition de l'INHES (Institut National des Hautes Études en Sécurité)

<sup>3</sup> Preparatory Action for Security Research - <http://europa.eu.int/comm/enterprise/security>  
<http://www.cordis.lu/security>.

<sup>4</sup> En particulier l'ESRAB, (European Security Research Advisory Board).

<sup>5</sup> Comme à l'occasion du colloque sur la recherche en sécurité organisé le 18 octobre 2005.

<sup>6</sup> Recherche planifiée ou enquête critique visant à acquérir de nouvelles connaissances, l'objectif étant que ces connaissances puissent être utiles pour mettre au point de nouveaux produits, procédés ou services ou entraîner une amélioration notable des produits, procédés ou services existants.

## 2- OBJECTIFS

### 2-1 : OBJECTIFS GENERAUX DE LA RECHERCHE EN SECURITE GLOBALE

La recherche en sécurité globale, est une recherche finalisée, capable de faire émerger des solutions concrètes face à des enjeux globaux sur le court, moyen et long terme. Pour ce faire, elle doit favoriser les approches systémiques, transverses et pluridisciplinaires en associant des partenaires industriels, académiques ainsi que les acteurs de la sécurité, qu'ils soient privés ou publics (prescripteurs et opérateurs).

Une approche systémique doit considérer les vulnérabilités et l'interdépendance des systèmes de plus en plus efficaces et complexes qui régissent les flux et infrastructures vitales nécessaires à nos sociétés, comme par exemple : les réseaux d'énergie, les réseaux informatiques, qui gèrent en particulier les flux financiers, traitent et diffusent l'information, les transports de personnes et de biens, les complexes industriels, les systèmes sanitaires, l'eau... L'approche système est également nécessaire vis-à-vis de la nature des solutions à apporter afin de proposer des concepts et architectures assurant la cohérence entre les phases de planification, de prévention, de surveillance, de détection, de gestion de la crise et de restauration de l'activité. Ces concepts et architectures doivent permettre d'orienter et de cibler des axes d'efforts technologiques et organisationnels essentiels au traitement des menaces et des risques (capteurs, traitement, intégration...).

La transversalité est nécessaire au regard de la diversité des acteurs, de l'hétérogénéité et du grand nombre des secteurs d'activités. Les défis imposés par les vulnérabilités pesant sur ces secteurs d'activité, de façon globale, réclament une meilleure synergie des acteurs afin de rationaliser les approches et démultiplier les efforts isolés.

La recherche en sécurité couvre par nature de très nombreux domaines et disciplines scientifiques qui sont appelés à concourir à l'amélioration de la sécurité (TIC, chimie, biologie, sciences cognitives, sciences sociales, ingénierie...) ainsi que les technologies émergentes susceptibles de générer de nouvelles solutions et vulnérabilités. L'approche transdisciplinaire recouvre également des travaux de nature collaborative permettant le rapprochement entre les sciences dites « dures » et les sciences humaines et sociales.

Une approche prospective, novatrice et structurée de la sécurité nécessite d'articuler efficacement la recherche amont et aval, dans l'objectif de fournir des solutions appliquées mais aussi applicables, tant du point de vue de l'acceptabilité des systèmes que de leur efficacité pratique et économique. En particulier il est absolument nécessaire d'anticiper les phases de certification et de normalisation des systèmes et équipements de sécurité. Une recherche partenariale, associant les acteurs de la recherche mais aussi les prescripteurs et opérateurs de la sécurité, permettra de déboucher sur des avancées significatives répondant aux attentes concrètes des citoyens.

La recherche en sécurité globale représente donc de très forts enjeux en terme d'innovation, de compétitivité économique et de souveraineté.

### 2-2 : OBJECTIFS DE L'APPEL A PROJET 2006

Le présent appel à projets vise à susciter une recherche scientifique et technologique de haut niveau, appelée à soutenir l'émergence d'une approche globale et systémique de la sécurité en favorisant les regroupements d'acteurs majeurs, académiques, industriels et d'utilisateurs finaux.

Il aura pour objectif également de préparer le tissu français de la recherche pour qu'il puisse se positionner sur les futurs appels à projets nationaux et européens. Dans cette optique, la durée maximale des projets sera de 36 mois.

Il s'attachera en particulier à identifier les lacunes des systèmes existants vis-à-vis des risques et menaces de toutes natures. Il devra permettre de proposer selon ce diagnostic, des axes d'amélioration organisationnels, sociologiques et technologiques, ainsi que des concepts de

prévention, de protection et de gestion de crise vis-à-vis de ces menaces. Des feuilles de routes pourront être proposées à l'issue de ces études.

Des résultats concrets sont également attendus sur la base de démonstration de faisabilité d'outils permettant :

- la gestion des alertes,
- la modélisation et la simulation visant à mieux analyser et gérer la complexité de la sécurité des systèmes ; l'aide à la décision ainsi que l'étude notamment rétrospective de la gestion d'une crise,
- le traitement de l'information : perception de la situation, fusion de données hétérogènes et exploitation de celles-ci.

Un volet sécurité et société devra permettre de mettre en évidence les enjeux et de proposer des axes d'efforts et des solutions dans les domaines de la recherche prénormative, de l'acceptabilité des acteurs vis-à-vis des systèmes de sécurité, ainsi que des aspects juridiques.

Pour l'appel à projets 2006, le niveau de démonstration attendu se limitera à la réalisation de plates-formes ou d'outils permettant de prouver la faisabilité des solutions proposées lorsque cela est pertinent. Compte tenu de la durée limitée des projets, le développement de briques technologiques particulières (par exemple les technologies de capteurs) et présentant un enjeu de recherche pour leur conception ne sera pas encouragé. Les démonstrations reposeront plutôt sur la mise en œuvre de briques technologiques existantes mais permettant d'extrapoler les besoins et spécifications ad hoc pour leur évolution lorsque cela sera jugé nécessaire.

Les recherches seront orientées selon des objectifs précis et appliqués à des cas concrets s'y rattachant. A titre d'exemple, on citera, dans le cadre de la lutte contre le terrorisme, la protection de sites et de moyens de transports appliquée à l'étude d'une grande gare routière ou ferroviaire.

Aucune priorité n'est donnée selon les différentes thématiques, mais le traitement de plusieurs thématiques est demandé (voir critères d'éligibilité). En particulier, la citation d'éléments d'analyse de vulnérabilité des systèmes considérés, si cette thématique n'est pas traitée dans le projet, comme données d'entrée en garantie de la crédibilité de celui-ci sera un des critères d'évaluation des projets (cf. § 4-3).

### **3- THEMATIQUES DE L'APPEL A PROJETS**

#### **T1 : L'ANALYSE DES VULNERABILITES DES SYSTEMES ET LES RISQUES, LEUR DEFINITION ET HIERARCHISATION.**

Cette analyse portera sur les aspects organisationnels, techniques et la relation entre les différents acteurs (cognitive, sociologique en particulier) et mettra en œuvre des méthodes innovantes.

Elle devra permettre de comprendre et diagnostiquer les forces et les faiblesses des systèmes selon :

- les types de risques potentiels,
- les modes organisationnels,
- les modes de définition des problèmes,
- les degrés de structuration des systèmes d'acteurs,
- les cadres cognitifs implicites,
- la nature des méthodes et outils mis en œuvre.

Ce diagnostic devrait permettre de mieux définir les risques et menaces, leur hiérarchisation (probabilité et impact) mais aussi de fournir des axes d'amélioration pour le système d'ensemble et/ou pour les autres thématiques de l'appel sous forme d'approches novatrices et/ou de données d'entrées (besoins d'outils ou aspects juridiques par exemples).

## **T2 : LA GESTION DES ALERTES**

La gestion des alertes recouvre d'une part la détection d'évènements significatifs et d'autre part les modes de diffusion et d'informations vers les acteurs avant et pendant la crise.

Pour la détection de signaux précurseurs, sont concernés :

- les techniques d'analyse sémantiques comme l'analyse de signaux faibles sur des sources ouvertes en particulier l'analyse automatisée des contenus des sites internet, blogs, chats ou fichiers texte,
- les méthodes et algorithmes d'extraction de données pertinentes au sein de données massives (images, vidéo, texte, son).

L'information des acteurs en temps de crise recouvre :

- la structuration des informations utiles entre les acteurs (contenu, niveau d'interprétation) tenant compte des facteurs interculturels et du besoin d'interopérabilité,
- la communication vers la population, par exemple en cas de crise grave, nécessitant des moyens et un contenu efficaces et cohérents avec les opérations en cours.

## **T3 : LES OUTILS DE MODELISATION, DE SIMULATION ET D'AIDE A LA DECISION.**

Les outils de simulation sont indispensables à l'élaboration des stratégies de préparation, de gestion et d'analyse de la crise dans toutes ses phases temporelles (avant, pendant et après) mais également à la meilleure définition et construction des systèmes de protection.

On distinguera :

- Les outils prédictifs nécessaires à la compréhension et l'analyse (entraînement par exemple) permettant :
  - ✓ la prise en compte des vulnérabilités et des scénarios complexes (juxtaposition des risques variés, effets dominos ou en cascade) et le recensement des modes opératoires associés,
  - ✓ l'intégration des modèles de comportement humain, de fonctionnement organisationnel par exemple en situation de stress (population et efficacité des intervenants dans leur environnement),
  - ✓ la prise en compte des phénomènes de propagation dans des milieux ouverts ou confinés (gaz toxiques, épidémies...),
  - ✓ l'entraînement interactif, distribué et représentatif des intervenants.
- Les outils permettant une meilleure représentation de la situation en particulier les Interfaces Homme - Organisation - Machine pour la visualisation de gestion de crise, incluant la représentation des environnements urbains.
- Les outils d'aide à la décision prenant en compte, dans une composante temps réel, les outils de planification ou de préparation mais également :
  - ✓ la gestion des tableaux de bords de gestion de crises,
  - ✓ l'exploitation de retour d'expérience et la confrontation avec les évènements en cours, en temps réel,

- ✓ l'étude des conditions de neutralisation, de réparation et d'un retour à la normale, recherches portant plus sur la résilience (architecture, redondance, substitution, subsidiarité, centralisation...).

#### **T4 : LE TRAITEMENT DE L'INFORMATION**

En complément ou en association avec les travaux sur la gestion de l'alerte (sur les aspects détection), ces travaux devront permettre l'étude d'architecture de plates-formes intégrées visant à améliorer :

- La perception d'une situation donnée (combinaison de menaces et de systèmes à protéger) en particulier :
  - ✓ l'étude des besoins humains, organisationnels et technologiques (capteurs chimiques, électroniques, neutroniques, optroniques, puces ADN, capteurs olfactifs, capteurs biométriques temps réel...),
  - ✓ leur action combinée et leur complémentarité,
  - ✓ leur disposition et leur mise en réseaux,
  - ✓ la sécurisation des informations issues de ces capteurs.
- L'architecture de traitement de l'information (répartition et gestion des flux de données entre les capteurs et les noeuds centraux, architectures ouvertes).
- La fusion de données d'origines hétérogènes, leur rapprochement et leur exploitation (échanges, partages, stockage...).

#### **T5 : SECURITE ET SOCIETE**

Les futures architectures de systèmes de sécurité ne pourront être introduites effectivement et efficacement sans une réflexion préalable sur leur pertinence du point de vue économique, sociologique et juridique.

- Une recherche prénormative visera à identifier les futurs systèmes de sécurité et cadres d'emploi de ces prénormes au moyen des outils d'intelligence économique et de prospectives. Des moyens méthodologiques pour y parvenir, comme la conception co-normative, seront également proposés.
- L'étude des phénomènes sociaux accompagnant l'introduction des nouveaux systèmes de sécurité :
  - ✓ étude de l'impact et de la perception des limites sociologiques à l'introduction des technologies et systèmes de sécurité dans tous les espaces de la vie publique et privée (créativité, acceptabilité du risque, prise de risque, esprit d'entrepreneuriat, cohésion sociale, exercice de la citoyenneté...),
  - ✓ recherche sur les systèmes d'informations et bases de données permettant le croisement d'informations sous contraintes de préservation des libertés individuelles (règles CNIL),
  - ✓ travaux sur le respect du caractère non invasif des méthodes d'identification biométriques (aspects éthiques).
- L'étude, l'analyse d'impact des évolutions juridiques et l'analyse comparée afin de mieux identifier les points d'application des nouveaux systèmes techniques et organisationnels :
  - ✓ recherche comparée avec d'autres pays en particulier anglo-saxons (liberté individuelle),
  - ✓ impacts du renforcement de l'arsenal juridique et législatif sur l'activité économique, les échanges commerciaux et l'économie numérique. Une étude sur le cas américain sur ce point est nécessaire pour analyser l'impact des mesures prises depuis « nine eleven » sur les échanges et les communications.

## 4- ELIGIBILITE DES PROJETS ET CRITERES DE SELECTION

### 4-1 PROCEDURE DE SELECTION

La procédure comprend successivement les étapes listées ci-dessous :

- Examen de l'éligibilité du projet et désignation des experts scientifiques par le comité d'évaluation ;
- Expertise scientifique des projets recevables par des experts extérieurs au comité d'évaluation ;
- Examen et classement des projets par le comité d'évaluation ;
- Sélection des projets par le comité de deuxième niveau ;
- Établissement de la liste des projets retenus et de la liste complémentaire par l'ANR ;
- Finalisation du dossier administratif et financier pour les projets retenus et les projets sur la liste complémentaire. En particulier une analyse de la capacité financière des entreprises sera effectuée pour le compte de l'ANR.

Les compositions du comité d'évaluation et du comité de deuxième niveau seront affichées sur le site internet de l'ANR ([www.agence-nationale-recherche.fr](http://www.agence-nationale-recherche.fr))

### 4-2 ÉLIGIBILITE DES PROJETS

Les projets éligibles devront

- Respecter le champ de l'appel à projets (en précisant les thématiques traitées) ;
- Aborder au moins deux thématiques parmi les cinq de l'appel à projets ;
- Correspondre à un projet de R&D en partenariat public/privé réunissant au moins un acteur du monde économique (industriels, opérateurs...) et un laboratoire académique ;
- Présenter une durée des travaux n'excédant pas 36 mois ;
- Être soumis dans les délais impartis, avec tous les documents ;

### 4-3 CRITERES D'EVALUATION ET DE SELECTION

Les propositions seront évaluées selon les six groupes de critères suivants :

#### **1 – Pertinence par rapport aux orientations de l'appel à projet**

- Le projet présente clairement :
  - ✓ les domaines de la sécurité globale abordés,
  - ✓ les vulnérabilité(s) du ou des système(s) nécessitant l'étude proposée, en mentionnant des études et/ou rapports qui serviront de données d'entrée au projet ou en abordant la thématique n°1 sur l'analyse de vulnérabilité,
- Le projet propose une approche système, pluridisciplinaire et multi-acteurs de la recherche en sécurité ;
- Le projet contribue :
  - ✓ à une meilleure compréhension des enjeux organisationnels, sociologiques ou technologiques de la sécurité,
  - ✓ à démontrer la faisabilité de méthodes, outils, validations ou démonstrations pertinents pour les systèmes de sécurité.

#### **2- Impact potentiel du projet**

- Le projet présente une véritable ambition :
  - ✓ de renforcement de la compétitivité industrielle française,
  - ✓ d'élargissement de la base de connaissances scientifiques, technologiques ou organisationnelles.

- Le projet a une stratégie convaincante en terme d'utilisation effective et de valorisation des résultats, en particulier vis-à-vis des opérateurs ou prescripteurs de la sécurité ;
- Le projet prend en compte les activités de recherche en cours dans le domaine de la sécurité et présente une réelle valeur ajoutée par rapport à elles ;
- La proposition identifie les éventuels problèmes d'ordre éthique et juridique induits par sa méthodologie ou ses objectifs.

### **3- Excellence scientifique et/ou technique**

- Le projet a des objectifs clairs contribuant effectivement à une meilleure sécurité des citoyens et/ou à la compréhension des enjeux organisationnels, humains et technologiques de la sécurité ;
- Les objectifs scientifiques et/ou techniques du projet représentent un réel progrès par rapport à l'état de l'art ;
- La démarche scientifique et/ou technique est adaptée aux objectifs poursuivis.

### **4- Qualité du consortium et du partenariat<sup>7</sup>**

- Les partenaires constituent collectivement un consortium de haute qualité et complémentaire ;
- Le partenariat présente effectivement les capacités et l'expertise requises pour la réalisation du projet ;
- Le consortium implique effectivement des opérateurs et/ou prescripteurs (publics ou privés) de la sécurité ;
- Le consortium implique un ou des acteurs industriels à même d'exploiter les résultats du projet ;
- La participation de PME/PMI sera appréciée.

### **5- Organisation et management du projet**

- L'organisation du projet est rationnelle et adéquate, compte tenu de la complexité du projet, du caractère novateur, de la qualification des partenaires et des résultats visés ;
- Le projet propose un plan de management cohérent et détaillé comportant en particulier une description du planning, des tâches, des jalons, des responsabilités des partenaires ainsi que des livrables ;
- Le projet propose une organisation du pilotage des travaux garantissant un démarrage effectif rapide à la notification du projet ;
- Le projet présente une stratégie en termes de gestion de la propriété intellectuelle et de gestion de la confidentialité des informations, des résultats et des livrables (en précisant les niveaux de diffusion de l'information).

### **6- Adéquation des moyens et des ressources**

- Le niveau de ressources proposé et détaillé (personnel, équipement, fonctionnement, ...) est adapté à la réalisation des objectifs du projet ;
- Le plan de financement est adéquat et garanti ;
- Le cas échéant le porteur de projet signale les sources de financements complémentaires déjà acquises au moment de la remise de la proposition.

**La méthode de notation** suivante sera appliquée :

<sup>7</sup> La labellisation par un pôle de compétitivité est considérée comme un indicateur de qualité. Elle est prise en compte dans le cadre de l'examen par le comité de deuxième niveau. Il est rappelé qu'il n'est pas nécessaire que tous les partenaires d'un projet soient membres du pôle ou localisés dans sa région pour que ce projet puisse bénéficier du label de "projet de pôle".



- Un projet est jugé par au moins 2 experts ;
- Chaque expert note de 0 à 5 les six critères d'évaluation décrits, commente et justifie sa notation ;
- Le comité d'évaluation, sur la base du rapport des experts attribue une note totale sur 30 points ;
- Une note inférieure ou égale à 2 sur un des critères est éliminatoire.

## 5- REGLES DE FINANCEMENT

D'une manière générale, ce sont les dispositions du règlement financier de l'ANR qui sont applicables (<http://www.agence-nationale-recherche.fr/documents/reglementANR.pdf>).

Les projets retenus dans le cadre du présent appel à projets seront financés par l'ANR. Le financement attribué sera apporté sous forme d'aide non remboursable.

Les aides de l'ANR ne pourront bénéficier qu'à des partenaires résidant en France. L'objectif de l'ANR est que la majorité des projets reçoivent un financement d'un montant compris entre 500 k€ et 1000 k€. Toutefois l'ANR n'exclut pas de financer des projets d'un montant inférieur ou supérieur. Par ailleurs, l'ANR n'attribuera pas d'aide d'un montant inférieur à 20 k€ à un partenaire d'un projet.

Pour les entreprises et les associations, le taux maximum d'aide de l'ANR (appliqué aux dépenses éligibles hors taxes) sera le suivant :

Type de recherche	Taux maximum d'aide pour les PME <sup>8</sup>	Taux maximum d'aide pour les entreprises autres que PME, et les associations
Recherche Industrielle <sup>9</sup>	60%	50%

Pour les organismes publics et les fondations de recherche, l'aide finance le coût marginal du projet. Il y a une exception à cette règle : pour les laboratoires des établissements publics à caractère industriel et commercial (EPIC) impliqués dans des recherches partenariales, l'ANR finance une partie du coût complet de l'opération.

Les dépenses sont calculées hors taxes, majorées le cas échéant, pour les laboratoires publics de recherche, de la TVA non récupérable.

Les bénéficiaires pourront commander des travaux à des tiers extérieurs (en France ou dans l'Espace Économique Européen) dans le respect des modalités fixées par le règlement financier de l'ANR.

Les dépenses relatives au recrutement de personnel sous contrat à durée déterminée (CDD) sont éligibles.

<sup>8</sup> Une PME est une entreprise comprenant jusqu'à 249 salariés, avec un chiffre d'affaires inférieur à 50 M€ ou un total de

bilan inférieur à 43M€. Les filiales de grands groupes ne sont pas considérées comme des PME.

<sup>9</sup> Recherche planifiée ou enquête critique visant à acquérir de nouvelles connaissances, l'objectif étant que ces connaissances puissent être utiles pour mettre au point de nouveaux produits, procédés ou services ou entraîner une amélioration notable des produits, procédés ou services existants.

## 6- CONFIDENTIALITE

Chaque porteur de projet pourra fournir une liste de 2 à 4 noms d'experts français (avec coordonnées jointes) susceptibles d'évaluer le projet. Il devra certifier sur l'honneur qu'il n'y a pas d'intérêt direct entre ces experts et les partenaires du projet.

Les porteurs de projets auront la possibilité de récuser (pour l'évaluation de leur projet) certains membres du comité d'évaluation ou des experts scientifiques (liste à fournir) s'il y a risque de conflit d'intérêts (contrats en cours, confidentialité, propriété intellectuelle).

Les membres du comité d'évaluation et du comité de deuxième niveau sont astreints à l'obligation de confidentialité.

Les projets devront mentionner explicitement le niveau de diffusion des différents documents, « délivrables » ou communications éventuelles (sous forme de tableau).

Il pourra être demandé au coordinateur du projet de présenter le rapport final lors d'une session orale qui réunira des membres de l'ANR, des évaluateurs chargés du suivi et des représentants des ministères concernés par les travaux.

## 7- POLES DE COMPETITIVITE

Le porteur de projet devra mentionner si le projet fait partie des projets labellisés (ou en cours de labellisation) par un pôle de compétitivité (ou par plusieurs, en cas de projet interpôles). Les partenaires d'un projet labellisé par un pôle de compétitivité et retenu par l'ANR dans le cadre de cet appel à projet pourront se voir attribuer un complément de financement par l'ANR.

Le porteur de projet devra fournir :

- la (les) attestation(s) de labellisation signée(s) par un (des) représentant(s) habilité(s) de la (des) structure(s) de gouvernance du (des) pôle(s) concerné(s) ;
- une fiche descriptive du projet (contenant au minimum le résumé du projet, le nom des partenaires, le montant total du projet et les financements demandés) visée par un (des) représentant(s) habilité(s) de la (des) structure(s) de gouvernance du (des) pôle(s) concerné(s).

Ces documents devront être transmis à l'Université de Technologie de Troyes (structure support de l'ANR pour cet appel à projets), dans un délai maximum de deux mois après la clôture de l'appel à projets, en exemplaire original par courrier (cachet de la poste faisant foi) et par courrier électronique.

**Faute de réception de ces documents dans les délais indiqués, aucun complément de financement ne sera accordé.**

## 8- MODALITES DE SOUMISSION

Le processus de sélection de cet appel à projets ainsi que l'évaluation et l'administration des dossiers de subvention ont été confiés à l'Université de Technologie de Troyes (UTT) par l'ANR.

L'ensemble des documents de l'appel à projets (texte, dossier de candidature et note synthétique) est accessible à partir de la page du présent appel à projets, sur le site web de l'ANR (<http://www.agence-nationale-recherche.fr>). Les personnes intéressées par le présent appel à projets sont donc invitées à consulter cette page sur le site web de l'ANR.

Le dossier soumis sous forme papier devra comprendre les mêmes éléments que le dossier complet électronique du projet. Les **versions "papier"**, signées, devront être envoyées en 3 exemplaires agrafés ou reliés, dont l'original.

Le **dossier sous forme électronique** devra impérativement être déposé avant le **mercredi 14 Juin 2006 (12h)** sur le site dédié : [www-anr\\_csosg.utt.fr](http://www-anr_csosg.utt.fr).

La réception des dossiers électroniques sera confirmée par courriel au coordinateur du projet qui se verra attribuer un numéro d'ordre par projet, sous 48 h ouvrés.

Le **dossier sous forme papier** devra être **posté** (pli recommandé avec accusé de réception) au plus tard le **jeudi 15 juin 2006 à minuit** (cachet de la poste faisant foi) à l'adresse suivante :

Université de Technologie de Troyes  
Appels à Projets ANR -CSOSG  
12, rue Marie Curie, BP 2060  
10010 Troyes Cedex.

Pour tout renseignement, les personnes à contacter sont les suivantes :

E. Châtelet – [ec.csosg@utt.fr](mailto:ec.csosg@utt.fr) -Tél : 0325715634  
Ph. Cornu – [phc.csosg@utt.fr](mailto:phc.csosg@utt.fr) - Tél : 0325715689

## **ANNEXE : TYPOLOGIE FONCTIONNELLE DE LA SECURITE<sup>10</sup>**

<b>Fonction</b>	<b>Description</b>
<b>Planification/préparation</b>	Analyses des risques, des vulnérabilités Planification des moyens, des évènements Exercice et Simulation (conception, déploiement, entraînement...) Formulation des besoins... Test, évaluations, certification
<b>Détection / identification / localisation</b>	Détection, identification d'explosifs, d'armes, Détection, identification, NRBC Détection humaine, sniper Détection d'intrusion Identification des personnes (biométrie,...) Positionnement, localisation Détection de situations et de comportements anormaux Détection environnementale
<b>Surveillance</b>	Surveillance aérienne Surveillance des approches maritimes Surveillance des frontières, de sites Surveillance de foule Surveillance, écoute des communications Surveillance des flux (contrôles, marquage, traçabilité...) Surveillance des flux immatériels (financiers...) Observation spatiale
<b>Protection</b>	Protection des personnes (y compris dans le cadre sécurité routière) Protection face aux explosifs et armes (personnes, sites, véhicule) Protection des systèmes d'information (dont réseaux bancaires), des systèmes de contrôles (SCADA) Protection des biens matériels et immatériels (y compris patrimoines numériques) Protection physique des sites sensibles Systèmes de contrôle des accès Réduction des caractères criminogènes Protection des réseaux d'eau potable et des chaînes alimentaires Protection face aux menaces NRBC (personnes, sites) Protection des transports
<b>Neutralisation</b>	Neutralisation NRBC Neutralisation d'armes Neutralisation de véhicule Neutralisation de personnes Brouillage des communications
<b>Opérations/gestions de crises</b>	SIC, interopérabilité, interconnexion,... SIG, aide à la décision Information, diffusion de l'alerte Réseaux d'alerte Soutien, secours et soin des populations
<b>Réparation</b>	Décontamination Dépollution Sauvetage Télémédecine Récupération de preuves
<b>Traitement de l'information</b>	Systèmes de télécommunications disponibles, sécurisées, durcies Fusion de données, Outils de veille (recherche et indexation, data mining, text mining) Traitements automatiques (reconnaissance de la parole, de l'image, des langues, traduction)
<b>Architecture des systèmes de sécurité</b>	Systèmes de contrôle des droits Systèmes de contrôle des positions et des déplacements Systèmes de protection Systèmes de renseignement Systèmes de surveillance et d'alerte Réseaux d'information

<sup>10</sup> Cette liste de fonctions, non exhaustive, est donnée à simple titre d'information. Les porteurs de projets ne sont d'aucune façon contraints d'y faire référence.