

La thématique Sécurité Globale dans le pôle SYSTEM@TIC PARIS-REGION

Dominique POTIER¹, Raymond FOURNIER², François CUNY¹

¹SYSTEM@TIC PARIS-REGION, 35 boulevard Nicolas Samson, 91120 Palaiseau

²CEA-LIST, Saclay, 91191 Gif-sur-Yvette Cedex

d.potier@systematic-paris-region.org, raymond.fournier@cea.fr, f.cuny@systematic-paris-region.org

Résumé – La Sécurité & Défense est un des cinq domaines de marché et de R&D portés par le Pôle de compétitivité mondial SYSTEM@TIC PARIS-REGION. Il rassemble 54 partenaires du Pôle dont 13 Établissements de recherche et/ou d'enseignement supérieur, 20 PME et 21 grandes entreprises. L'article introduit d'abord la vision et les priorités du Pôle en matière de Sécurité & Défense et les illustre ensuite par quelques exemples de projets de R&D en cours. Il présente ensuite les principaux clusters existants au niveau mondial dans le domaine de la sécurité et conclut sur les enjeux et perspectives à moyen-terme en matière de plate-formes et de partenariats internationaux.

Abstract – Security & Defence is one of the five business domains and R&D themes that are developed by the world-class cluster SYSTEM@TIC PARIS-REGION. It gathers 54 industrial and academic members from the Paris-Region who work in partnership on R&D and business developments projects for the Security & Defence markets. In this paper, we introduce the strategy and research priorities of the Pôle for the domain of Security & Defence and illustrate them by examples of on-going R&D projects. We then give a brief survey of the main clusters dedicated to Security & Defence around the world and conclude by presenting our mid-term challenges in term of platforms and international partnerships.

1. SYSTEM@TIC PARIS-REGION

1.1. Les pôles de compétitivité : définition et contexte

Face à l'accélération des mutations économiques internationales et à l'émergence de nouveaux compétiteurs de poids sur la scène internationale, la France a décidé en 2004 de mettre en place une politique industrielle volontariste misant sur l'innovation et le développement de la R&D, facteurs clés de la compétitivité industrielle.

Dans ce contexte concurrentiel, la mobilisation forte des acteurs territoriaux et le développement des synergies locales entre l'industrie, la recherche et la formation sont identifiés comme des éléments importants de la compétitivité industrielle.

En septembre 2004, le Comité Interministériel de l'Aménagement et du Développement du Territoire (CIADT) décide de mettre en place cette nouvelle politique industrielle à travers un appel à propositions de pôles de compétitivité.

Le concept de pôle de compétitivité reprend celui de cluster introduit par Michael E. Porter et défini comme

suit : « *Clusters are geographic concentrations of interconnected companies, specialized suppliers, service providers, firms in related industries, and associated institutions (e.g., universities, standards agencies, trade associations) in a particular field that compete but also cooperate* » [1].

Un pôle de compétitivité se définit donc comme la combinaison, sur un territoire donné, d'entreprises, de centres de formation et d'unités de recherche publiques et privées, engagés dans une démarche partenariale destinée à dégager des synergies autour de projets communs au caractère innovant, et disposant de la masse critique nécessaire pour une visibilité internationale [2]

1.2. SYSTEM@TIC PARIS-REGION : le Pôle dédié à la révolution numérique

Au cœur de la révolution numérique, le Pôle de compétitivité mondial SYSTEM@TIC PARIS-REGION fédère plus de 250 acteurs industriels, académiques et institutionnels franciliens autour de projets de R&D coopératifs et d'actions de développement ciblés sur cinq marchés à forte valeur ajoutée: Télécommunications, Sécurité & Défense, Automobile & Transports, Outils de Conception et Développement de Systèmes et depuis octobre 2007 le Logiciel Libre (sur la base de l'initiative

"Ouverture" portée par les acteurs du logiciel libre en Ile-de-France).

Sur ces thématiques, la mission de SYSTEM@TIC PARIS-REGION est le développement de l'économie, de la compétitivité des entreprises et de l'emploi en utilisant les leviers de l'innovation, de la formation et du partenariat. Les acteurs du Pôle (chercheurs, industriels, organismes de formation et collectivités territoriales) se sont fixés trois objectifs prioritaires :

- Consolider le leadership des grands intégrateurs pour ancrer durablement leurs activités de R&D en Ile-de-France.
- Contribuer à l'émergence de nouvelles sociétés et au développement de PME technologiques à vocation mondiale.
- Renforcer l'attractivité de l'Ile-de-France en la dotant d'une image technologique visible au niveau international afin d'attirer les centres de R&D de nouvelles entreprises mondiales.

1.3. Une organisation associant marchés technologiques et marchés sectoriels

Le positionnement du Pôle se situe à la croisée de marchés sectoriels (Télécommunications, Sécurité & Défense, Automobile & Transports) et de marchés technologiques (Outils de Conception et Développement de Systèmes, Logiciels Libres). Ce positionnement est porté et développé par une organisation structurée en **5 Groupes Thématiques** au sein desquels les acteurs du Pôle définissent leurs visions stratégiques et élaborent les projets de R&D coopératives et les actions de développement.

Tableau 1 : Groupes Thématiques du Pôle

1. Automobile & Transports
2. Télécoms
3. Sécurité & Défense
4. Outils de Conception et Développement de Systèmes
5. Logiciel Libre

2. Le Groupe Thématique "Sécurité & Défense"

Pour une forte part, les technologies à l'origine de la révolution numérique ont émergé et se sont développées au cours de la seconde moitié du 20^{ème} siècle en réponse aux enjeux des secteurs de la défense et de la sécurité. L'activité du Groupe Thématique Sécurité & Défense [3] se situe très directement dans cette évolution. Mais elle vise aussi à répondre aux vulnérabilités nouvelles liées au déploiement des grands systèmes à bases de TIC (Technologies de l'information et de la Communication) qui assurent la conduite et la gestion de pratiquement toutes les activités de nos sociétés.

Avec 54 partenaires dont 13 Établissements de recherche et/ou d'enseignement supérieur, 20 PME et 21 grandes entreprises, le Groupe Thématique Sécurité & Défense du pôle de compétitivité SYSTEM@TIC PARIS REGION rassemble aujourd'hui une capacité de R&D organisée et focalisée sur la résolution des enjeux de

sécurité. Cette capacité est sans équivalent en France et, à notre connaissance, en Europe.

Ces capacités de R&D et de développement économique sont mises en œuvre en association étroite avec les acteurs qui définissent et portent les enjeux de la sécurité:

- Les autorités publiques qui définissent les politiques de sécurité et en contrôlent la mise en œuvre
- Les opérateurs de services au sens large (administrations, collectivités locales, transports, énergie, commerce, ...) qui déploient des systèmes de sécurité.

2.1. Nouveaux défis

Citoyens, entreprises, responsables institutionnels, politiques et gouvernementaux doivent faire face à un ensemble de risques nouveaux (risques techniques et catastrophes naturelles, terrorisme et cyber-terrorisme, etc.) amplifiés par les évolutions majeures de nos sociétés : développement des mégapoles, généralisation du e-commerce et de l'e-gouvernement, mondialisation des échanges de personnes et de services, etc.

Ces risques sont notamment liés à :

- La concentration de grands ensembles de personnes (lieux publics, gares, aéroports) : à titre d'exemple, trois milliards de passagers transitent annuellement dans les 30 plus importants aéroports du monde.
- La dépendance croissante de la société sur des infrastructures techniques et des réseaux complexes (dans les domaines de la santé, de l'industrie, des transports, du commerce, de la finance, etc.).
- La dématérialisation des activités et des relations sous la forme d'échanges électroniques (commerce, finance, etc.). Leur développement repose entièrement sur la capacité des technologies mises en œuvre à créer la confiance des opérateurs et usagers.

Ces risques sont particulièrement importants dans les régions à forte densité de population et d'activité. C'est le cas de l'Ile-de-France où se concentrent centres de décision, sites industriels, réseaux, nœuds de transports, infrastructures financières, irrigués par une population de plus de 5 millions de personnes en mobilité quasi-permanente. Ces risques de sécurité ne pourront être traités sans des innovations significatives en matière de technologies numériques et d'architecture de grands systèmes complexes.

2.2. La réponse du Groupe Thématique

Le Groupe Thématique Sécurité & Défense du pôle a décidé de focaliser son activité sur 2 grands axes stratégiques :

- Sécurisation des infrastructures critiques : transports, énergie, centres de décision, sites de loisirs, etc.
- Sécurité des systèmes d'information (SSI) : e-gouvernement, e-commerce, communication, identité numérique

Dans ce contexte, les axes de recherche et d'expérimentation du Groupe Thématique du marché Sécurité & Défense se concentrent sur trois priorités :

- Accroître la sécurité opérationnelle en innovant en termes de systèmes et d'équipements : protection d'infrastructures critiques, gestion de crise, etc.
- Sécuriser les systèmes d'information sensibles grâce aux nouvelles technologies et méthodes de preuve de confiance
- Mutualiser le développement des technologies critiques numériques et logicielles pour une réponse duale aux besoins civils et de défense

3. Vision et projets sur la Sécurité Globale

La vision et les priorités de R&D du Groupe Thématique sont analysées et revues annuellement selon la segmentation suivante :

1. Systèmes pour la sécurité des biens et des personnes
2. Technologies de sécurité physique
3. Systèmes de confiance numérique
4. Technologies de SSI

Les conclusions de ces analyses sont essentielles pour orienter le montage des projets nouveaux et pour leur cohérence globale. Elles font par ailleurs l'objet d'un rapport [4] transmis à l'ANR (Agence Nationale de la Recherche) avec l'objectif d'assurer la meilleure cohérence entre les orientations de ses programmes de recherche concernés et les projets de développement du Groupe Thématique. En 2007, les programmes de l'ANR principalement concernés étaient :

- Le programme Concepts, Systèmes et Outils pour la Sécurité Globales (COSG) pour les segments 1 et 2 du Groupe Thématique.
- Les programmes Sécurité et Sûreté Informatique (SeSur), Technologies Logicielles (TechLog) et Télécommunications pour les segments 3 et 4.

L'effort de R&D aujourd'hui investi dans les projets du Groupe Thématique par l'ensemble des partenaires représente plus de 130 M€ pour l'ensemble des 24 projets engagés depuis 2006 dont plus de 71 M€ dédiés aux 16 projets sur la sécurité globale.

Les 24 projets du Groupe Thématique sont soutenus pour 9 d'entre eux par le FUI (Fond Unique Interministériel) et les collectivités territoriales et pour les 15 autres par l'ANR.

Nous donnons dans la suite un rapide aperçu de 3 des 16 projets de l'axe stratégique Sécurité Globale :

- Sécurisation des Infrastructures Critiques (SIC) ;
- eXtended-Vision (X-Vision) ;
- Technologie pour l'Apprentissage des Risques majeurs par l'ANimation de Simulations (Taranis).

3.1. Le projet SIC

Le projet SIC (Sécurisation des Infrastructures Critiques) est un projet fédérateur sur le thème de la

sécurisation des infrastructures critiques. Il vise à développer les solutions (aspects système et technologique) nécessaires pour faire face aux menaces présentes et futures. Les travaux consistent en :

- une étude système visant à établir les besoins et définir les solutions ;
- des premiers développements technologiques qui seront expérimentés sur 2 sites (une préfecture et une gare) ;
- une roadmap des travaux supplémentaires à prévoir.

Ce projet est mené en coordination avec les opérateurs d'infrastructures critiques de la région parisienne et les autorités de tutelle, tout en restant cohérent avec les initiatives européennes dans le cadre du PERS.

Les principaux défis de ce projet sont de :

- définir les technologies nécessaires pour sécuriser les infrastructures critiques à partir d'une étude système centrée sur les besoins opérateurs ;
- développer des premières maquettes de briques technologiques (capteurs, middleware, logiciels de tenue de situation) cohérentes avec une démarche d'ensemble visant à équiper tous types d'infrastructures ;
- mener deux expérimentations à l'intérieur d'infrastructures opérationnelles afin de valider la démarche système retenue et les premières briques technologiques disponibles.

Porté par Thales, ce projet rassemble 18 partenaires du pôle qui vont investir près de 25 M€ sur 48 mois pour se placer dans la compétition mondiale de la sécurité globale.

3.2. Le projet X-Vision

Le projet eXtended-Vision (XVISION) vise à étudier et développer des caméras (analogiques dans un premier temps, puis numérique) en utilisant un nouveau capteur CMOS innovant qui garantit le maintien de la visibilité et des contrastes même dans des situations où la luminosité est difficile (conjonction de points très brillants, zones sombres). En parallèle du développement des caméras, ce projet se donne pour objectif d'étudier et de réaliser des adaptations sur les logiciels de traitement d'image. Les expérimentations seront menées dans les domaines de la surveillance périmétrique des sites sensibles et des transports publics urbains.

Porté par la société CEDIP, ce projet rassemble 7 partenaires avec un investissement de R&D de 2 M€ sur 18 mois pour développer et valider les concepts des nouvelles caméras et en préparer la mise sur le marché.

3.3. Le projet TARANIS

Le projet TARANIS – Technologie pour l'Apprentissage des Risques majeurs par l'ANimation de Simulations – est l'un des 15 projets du Groupe Thématique "Sécurité & Défense" soutenus par l'ANR (Agence Nationale de la recherche) dans le cadre du programme Concepts, Systèmes et Outils pour la Sécurité Globale.

Le projet TARANIS a pour objectif la réalisation d'une plate-forme générique permettant l'entraînement de cellules de crises à l'aide de technologies de simulation. A la différence des exercices classiques, il s'agit de restituer la complexité d'une crise survenant sur un site industriel afin d'immerger les équipes entraînées dans un environnement réaliste et dynamique. TARANIS fournira l'infrastructure logicielle générique permettant la réalisation de tels entraînements.

TARANIS offre ainsi un outil d'entraînement à la gestion de crise adaptée aux décideurs (élus locaux, préfets, responsables opérationnels...) qui doivent faire face à des risques croissants, des systèmes de plus en plus complexes et une multiplicité des acteurs.

Les principaux avantages du système sont les suivants :

- Plate-forme générique facilement déployable et configurable.
- Mise en œuvre d'une technologie de simulation d'une situation de crise virtuelle intégrant les risques technologiques et environnementaux, le comportement des populations et la simulation des primo-intervenants.
- Présence d'outils d'aide au débriefing.
- Intégration aux systèmes opérationnels.

Porté par MASA Groupe, le projet TARANIS rassemble les 3 partenaires MASA, ESRI France et le LRI (Laboratoire de Recherche en Informatique CNRS - Université Paris-Sud) qui vont engager près d'un million d'euros sur 2 ans pour atteindre les objectifs de ce projet.

4. La dimension internationale

Les événements récents de notre environnement, tels que les catastrophes naturelles et le terrorisme international, ont conduit à élargir le concept de sécurité et ont montré que l'innovation est essentielle pour faire face au caractère évolutif de ces menaces. Ce que l'on peut tenir aujourd'hui pour acquis est aussi la persistance de la menace sur la durée : l'évolution estimée du besoin de contrôle des passagers entre 2006 et 2016, présentée dans le tableau ci-dessous, est à elle seule suffisante pour s'en convaincre :

Tableau 2 : contrôle des passagers aériens

Marché du contrôle de passagers		2006	2016
Aéroports			
Nombre de postes de filtrage	Total France	200	325
	Total Europe	1 400	2 100
Transports publics (Métro, Tram, Bus)			
Nombre de points de contrôle	Total France	24 000	56 000
	Total Europe	240 000	560 000

Un autre caractère important de la menace est son caractère international qui amène de nombreux pays à organiser une réponse au sein de leur industrie et de leur recherche et le cas échéant à collaborer avec leurs voisins.

On ne reviendra pas ici sur les investissements importants consentis aux USA sur le « Homeland Security », mais il est intéressant de constater que de nombreux autres pays considèrent le domaine de la sécurité globale comme un secteur économique appelé à une croissance durable.

C'est le cas par exemple en Europe avec le programme de la Commission européenne "Prevention, preparedness and Consequence management of Terrorism and other security related risks" qui a fait l'objet de premiers appels à projets en 2007.

Nous présentons brièvement ci-dessous quelques exemples d'initiatives de types « cluster » en cours en Amérique du Nord et en Europe.

4.1. Canada (Ontario) : Ottawa Security Cluster

La région d'Ottawa abrite plus de 200 entreprises employant de plus de 20 000 personnes, ainsi que la Défense nationale, la Gendarmerie royale du Canada, la Sécurité publique et la Protection Civile du Canada. La base industrielle est soutenue par le Defence Research Establishment Ottawa, le Centre de recherches sur les communications, le Centre canadien de recherches policières et deux universités.

Le « Ottawa Security Cluster » [5] vise à développer le potentiel économique de croissance de la région. Les produits, services et domaines d'expertise comprennent entre autre :

- capteurs et technologies pour la surveillance
- systèmes de commandement et de contrôle (C4ISR)
- interopérabilité des communications
- véhicules et robotique autonome,
- applications liées à la sûreté du transport, les premiers intervenants, et de la sûreté portuaire,
- conception des véhicules terrestres, les sous-systèmes, de fabrication et de soutien
- véhicules aériens ; fabrication et maintenance,
- sécurité des systèmes d'information
- solutions de protection personnelle
- solutions de sécurité physique

4.2. Canada (Québec) : Technopôle Défense et Sécurité

Le Technopôle Défense et Sécurité (TDS) [6] est un réseau d'affaires dans les secteurs de la défense, de la sécurité et de la protection civile. Branché sur les besoins des clients, le TDS forme des partenariats stratégiques associant l'expertise et les ressources de ses membres afin d'accélérer l'adoption de solutions intégrées sur le marché de la défense et de la sécurité. Les marchés sectoriels visés sont :

- Défense :
 - Commandement, contrôle, communication, informatique, information, surveillance et reconnaissance (C4ISR)
 - Protection de la force
 - Systèmes d'armes

- Sécurité publique et protection civile:
 - Coordination et interopérabilité
 - Protection des infrastructures essentielles
 - Prévention du crime et maintien de l'ordre
 - CBRN
 - Surveillance et contrôle des frontières et traçabilité
 - Sécurité des grands événements
 - Biométrie

Le TDS s'organise autour d'un Centre d'intégration technologique, d'un Campus industrie/recherche, d'un Bureau de commercialisation et d'intelligence des marchés, et veut offrir un portefeuille technologique complet, visible et cohérent.

4.3. Suède: Knowledge to Safeguard Security

Ce programme de recherche national, « Connaissances pour garantir la sécurité » [7], vise à structurer la recherche suédoise et contribuer à la fois à augmenter la sécurité en suède et ses voisins, et à fournir le socle d'une croissance économique durable en permettant à la recherche et à l'industrie suédoise de prendre une place significative dans les réseaux internationaux. Les priorités identifiées :

1. Une coordination unifiée de la recherche sur la sécurité,
2. Etre proactif dans le programme PERS du FP7,
3. Participer aux programmes US de R&D en sécurité,
4. Créer des approches innovantes pour la sécurité.

4.4. Allemagne: Research for Civil Security

Le Ministère Fédéral de la Recherche et de l'Education (BMBF) a mis en place en 2007 son premier programme de recherche en matière de sécurité civile [8]. "No chance for crime or terrorism" et "Using research to protect freedom" forment, avec les aspects économiques associés, les bases de la vision allemande de la recherche dans le domaine de la sécurité. La prévention et l'innovation technologique sont vus comme des moyens possibles de réagir rapidement et globalement aux crises et de réduire sensiblement les effets des attaques, incidents informatiques et même catastrophes naturelles. Ces nouvelles solutions de sécurité pour les réseaux de communication, les installations industrielles, les bâtiments, les services publics et les systèmes de logistique doivent les rendre plus robustes et moins attrayants pour les attaquants. L'innovation technologique pour la sécurité offre également des possibilités de croissance économique:

En Allemagne, la croissance rapide du marché des produits et services de sécurité a généré 10 milliards € de chiffre d'affaires en 2005. La sécurité des TIC représentait 3,6 milliards € de ce montant. Le BMBF considère ainsi que ne pas s'engager pas dans le domaine de la technologie de la sécurité civile c'est refuser d'énormes possibilités dans les grands marchés de demain. Stratégiquement, la participation de l'Allemagne au programme PERS de l'EC est jugée comme essentielle.

4.5. Allemagne: Fraunhofer Innovation Cluster "Future Security BW"

L'objectif du cluster Future Security BW [9] est le développement de mesures techniques innovantes pour la sécurité de la population et des infrastructures critiques en vue de la menace terroriste. Ce cluster regroupe 22 entreprises, 10 instituts de recherche dont 6 Fraunhofer, et 3 universités du Bade-Wurtemberg, ainsi que 8 institutionnels et end-users de la sécurité.

Il a été créé au 2^{ème} trimestre de 2007, pour une durée de 5 ans au moins.

Le volume de projet visé pour ce Cluster est de 5-7 millions € / an, financés par contrats industriels, subventions (Etat fédéral, gouvernement fédéral, UE), l'organisation Fraunhofer et les ressources propres des instituts participants. Les principaux domaines techniques sont :

- Infrastructures Critiques : Murs instrumentés robustes ; Capteurs intégrés dans les matériaux de structure, nouvelles protections.
- Détection et identification des substances biologiques et explosives, bio-protection.
- Intégration des systèmes de sécurité ; Système de guidage de sécurité.
- Sécurité et société : Les aspects sociaux limitent la demande et les possibilités de recherche. Des études éthiques, juridiques, socio-économiques, psychologiques, visent à définir les conditions d'acceptation de la technologie et des produits.

5. Conclusions et perspectives

Avec moins de deux ans et demi d'existence, le Pôle de compétitivité SYSTEM@TIC PARIS-REGION et sa thématique Sécurité & Défense sont encore en phase de croissance et de structuration. Pour les prochaines années, deux des enjeux principaux sont :

1. La mise en oeuvre d'une politique de plate-formes.
2. Le développement de partenariats internationaux.

5.1. Plate-formes

Pour le Pôle SYSTEM@TIC PARIS-REGION les objectifs d'une plate-forme sont, pour ses thèmes de R&D majeurs, de capitaliser dans la durée les résultats des projets conduits autour de ce thème et de permettre une mutualisation des ressources et outils nécessaires à son développement (expérimentation et validation de technologies, démonstrations réalistes, accueil d'experts internationaux, conférences et séminaires). Un critère déterminant d'établissement d'une plate-forme est celui de sa viabilité économique : une plate-forme doit démontrer sa capacité à financer son fonctionnement et son développement par la fourniture de services aux partenaires du Pôle.

Pour la thématique Sécurité & Défense, les projets de plate-forme suivants sont en cours de préparation :

- Plate-forme Capteurs Vision : cette plate-forme, élaborée conjointement avec la thématique

Automobile & Transport, a pour finalité la conception et la validation de chaînes de vision temps-réel embarquées.

- Plate-forme SIC (Sécurisation des Infrastructures Critiques) : en prolongement du projet SIC présenté en 3.1, la plate-forme SIC vise à constituer les acquis de ce projet en centre de ressources et de démonstration au service d'une part des industriels, d'autre part des autorités et des opérateurs de sécurité.

[9] *Future Security BW. Protection, sensor technology, system integration, society.* Fraunhofer Gesellschaft, 2007

5.2. Partenariats internationaux

Le développement du Pôle de compétitivité mondial SYSTEM@TIC PARIS-REGION passe également par l'établissement de partenariats avec des initiatives de type cluster au niveau international. A travers ces partenariats, il s'agit de passer d'un modèle de coopération en réseaux de partenaires larges et fortement évolutifs, tel que mis par exemple en œuvre dans les projets de R&D coopérative de la Commission européenne, à un modèle de partenariats stables associant un nombre réduit de clusters dédiés à une même thématique.

Un premier exemple de ce type de partenariat inter-cluster du Pôle a été mis en place par le groupe thématique Automobile & Transport avec le cluster SafeTRANS en Allemagne du Nord consacré aux problématiques de sécurité dans les transports.

Pour la thématique Sécurité & Défense, l'objectif dans les prochaines années est d'établir ce type de partenariats avec un ou plusieurs des clusters dédiés à la sécurité tels que ceux qui ont été présentés en 4. De ce point de vue, la décision prise en 2007 par le BMBF en Allemagne et l'ANR de coordonner l'action des instituts Fraunhofer allemands et des instituts Carnot français dans cinq domaines de recherche dont la sécurité civile va contribuer de façon directe à cet objectif.

Références

- [1] Michael E. Porter. *Location, Competition, and Economic Development: Local Clusters in a Global Economy*, *ECONOMIC DEVELOPMENT QUARTERLY*, 14, p. 16
- [2] Voir www.competitivite.gouv.fr
- [3] Dominique Potier. *Zoom sur la thématique "Défense & Sécurité"*, SYSTEM@TIC Newsletter, n° 4, juin-juillet 2005.
- [4] *Défis et thèmes de recherche du pôle System@tic Paris-Région.* SYSTEM@TIC PARIS-REGION, septembre 2006.
- [5] Voir www.securitycluster.com
- [6] Voir www.technopoleds.org
- [7] *Knowledge to safeguard security. Proposals for a national strategy for security research.* Swedish Agency for Innovation Systems, June 2005
- [8] *Research for civil security. Programme of the German Federal Government.* Federal Ministry of Research and Education, Bonn, Berlin 2007.