

La vidéosurveillance intelligente : promesses et défis

Rapport de veille technologique et commerciale



Valérie Gouaillier
CRIM

Aude-Emmanuelle Fleurant
Technopôle Défense et Sécurité

Mars 2009
Mise à jour 8 avril 2009

Centre de recherche informatique de Montréal

550, rue Sherbrooke Ouest, bureau 100
Montréal (Québec) H3A 1B9

Technopôle Défense et Sécurité

Bâtiment 200, Site Sud - RDDC Valcartier
2459, boul. Pie-XI Nord
Québec (Québec) G3J 1X5

Ce rapport de veille a été réalisé grâce
à l'appui financier d'Industrie Canada



**Industrie
Canada**

**Industry
Canada**

et du Ministère du Développement économique, de l'Innovation et
de l'Exportation du Québec, principal partenaire financier du CRIM



Mot d'ouverture

Le Centre de recherche informatique de Montréal (CRIM) et Technopôle Défense et Sécurité sont fiers de vous présenter ce rapport de veille dressant un portrait de la technologie de la vidéosurveillance intelligente pour la sécurité des personnes et des lieux, ainsi que du marché en pleine croissance qu'elle représente.

Au cours de la dernière décennie, la sécurité des personnes, des biens et de l'information s'est imposée comme un enjeu majeur à l'échelle planétaire. Confrontées à des problèmes tels que la lutte au terrorisme, le renforcement de la sécurité intérieure et l'essor de la cybercriminalité, nos sociétés investissent de plus en plus pour assurer leur protection. Ce secteur offre donc de grandes opportunités pour les entreprises, tant sur le plan du développement technologique que des services. En particulier, les technologies de l'information et des communications apportent des solutions nouvelles et sophistiquées pour la sécurité physique et informatique.

Parmi les solutions proposées, la vidéosurveillance constitue l'une des technologies de sécurité les plus anciennes et répandues. Bien qu'encore principalement analogique, elle connaît une révolution numérique avec le passage amorcé à la vidéo sur réseaux IP. Intégrant parfois des centaines de caméras, ces nouveaux systèmes génèrent une quantité colossale d'informations vidéo qui dépassent les capacités de surveillance des agents de sécurité. Pour résoudre ce problème, la vidéosurveillance intelligente, par l'analytique vidéo, permet de traiter, de façon logicielle, la vidéo captée pour n'en retenir que les données pertinentes pour la sécurité.

La vidéosurveillance en est donc à un point tournant. Que représente le virage IP et quel est le potentiel de l'analytique vidéo ? Ce rapport de veille, s'adressant à un public non expert, couvre les principaux aspects de la question : applications, techniques de pointe en analytique vidéo, besoins des utilisateurs, développements et tendances dans ce domaine, principaux joueurs et marché de la vidéosurveillance, particulièrement au Québec.

Point convergeant de recherches en TIC menées par le CRIM et en sécurité menées par Technopôle Défense et Sécurité, la vidéosurveillance intelligente constituait une thématique des plus porteuses pour réaliser conjointement un premier rapport. Pour les entreprises et les chercheurs québécois spécialisés en TIC, ce secteur émergent offre de nouvelles opportunités, tant sur le plan du développement technologique que des services qu'il nous importait de circonscrire et de diffuser.

TDS a fait appel au CRIM pour mener cette veille sur la base de son expertise en vidéosurveillance. En effet, l'équipe Vision et imagerie de la division R-D du CRIM est impliquée dans ce secteur depuis 2003, à travers différents mandats multipartenaires. Mentionnons, par exemple, les projets suivants :

- *Monitoring of Extended Premises - Tracking Pedestrians Using a Network of Loosely Coupled Cameras (projet MONNET)*. Mis en œuvre par le Laboratoire de vision et systèmes numériques de l'Université Laval, ce projet avait pour but de développer un système intelligent de vision pour la surveillance de personnes dans des endroits publics. L'équipe du CRIM a contribué au niveau du module de reconnaissance de visages et d'expressions faciales. Ce projet était financé en partie par le programme de Precarn visant la recherche pilotée par les universités (PUL). Ce projet a remporté le Prix de la meilleure démo à la conférence annuelle IS-2005 de Precarn.
- *Intelligent Pan/Tilt/Zoom Camera for Security Applications (projet PTZ)*. Mis en œuvre par la firme VideoWave Networks, ce projet visait le développement d'une caméra Pan/Tilt/Zoom intelligente pour des logiciels de surveillance vidéo. L'équipe du CRIM était partenaire pour le développement et l'implémentation des algorithmes de suivi et reconnaissance d'objets. PTZ a été financé en partie par le Programme Alliance Precarn-CRIM. Ce projet a remporté le Prix OCTAS de l'innovation technologique 2006, décerné conjointement à VideoWave Networks et au CRIM par la Fédération de l'informatique du Québec.
- *Video Scene Understanding for the VST OneTrack System (projet VISU)*. Ce projet vise le développement d'une version avancée du module intelligent d'analyse de scènes développé dans le cadre du projet PTZ. L'équipe du CRIM est responsable, entre autres, de développer et tester des algorithmes de comptage de piétons et de détection de situations anormales des tracés de voitures. Ce projet est aussi financé en partie par le Programme Alliance Precarn-CRIM.

Jumelé avec l'explosion d'activités dans le secteur de la vidéosurveillance, l'idée de procéder à une veille stratégique circulait au CRIM depuis 2007. Grâce au support financier de Industrie Canada, TDS et le CRIM ont finalement pu réaliser le présent rapport.

Nous souhaitons adresser nos plus sincères remerciements à chacun des collaborateurs à cette étude ainsi qu'à nos partenaires gouvernementaux. Votre judicieux apport a rendu possible la concrétisation de ce projet.

Alain Fecteau

Président-directeur général
Technopôle Défense et Sécurité

Jacques Ouellet

Premier vice-président, R-D et commercialisation
CRIM

TABLE DES MATIÈRES

MOT D'OUVERTURE.....	3
TABLE DES MATIÈRES.....	5
RÉSUMÉ EXÉCUTIF.....	9
INTRODUCTION	11
REMERCIEMENTS	12
1. DÉFINITION DU DOMAINE	14
1.1 Sécurité	14
1.2 Vidéosurveillance	15
1.3 Vidéosurveillance intelligente	17
1.3.1 Raisons pour l'utilisation de vidéosurveillance intelligente	17
1.3.2 Facteurs déterminant le choix d'un système de vidéosurveillance intelligente	19
2. SECTEURS D'APPLICATIONS.....	19
2.1 Gouvernement et sécurité publique	20
2.2 Éducation	21
2.3 Commerce de détail	22
2.4 Transports.....	23
2.4.1 Aéroports.....	23
2.4.2 Gares et transports publics	24
2.4.3 Ports.....	25
2.5 Milieu bancaire	25
2.6 Industrie du jeu et casinos	25
2.7 Autres	26
3. TECHNOLOGIE	26
3.1 Architecture des systèmes de vidéosurveillance.....	26

3.1.1	Composantes d'un système de vidéosurveillance.....	26
3.1.1.1	Acquisition.....	26
3.1.1.2	Transmission	27
3.1.1.3	Compression.....	28
3.1.1.4	Traitement.....	29
3.1.1.5	Archivage	29
3.1.1.6	Affichage	30
3.1.2	Évolution des systèmes de vidéosurveillance	31
3.1.2.1	Première génération : le tout analogique.....	31
3.1.2.2	Deuxième génération : le système hybride	32
3.1.2.3	Troisième génération : le tout numérique IP.....	33
3.1.3	Vidéosurveillance IP.....	34
3.1.4	Architecture d'un réseau de vidéosurveillance intelligente	36
3.1.4.1	Architecture centralisée	37
3.1.4.2	Architecture distribuée	37
3.2	État de l'avancement technologique en analytique vidéo	37
3.2.1	Description des techniques d'analytique vidéo.....	38
3.2.1.1	Détection de changements	39
3.2.1.2	Suivi d'objets.....	41
3.2.1.3	Classification et identification d'objets	42
3.2.1.4	Classification d'activités et de comportements.....	44
3.2.1.5	Analyse de foule	45
3.2.1.6	Vidéosurveillance active dans les systèmes multi-caméras.....	46
3.2.2	Analytique dans les systèmes commerciaux.....	47
3.2.3	Besoins et défis en analytique vidéo	49
3.3	Tendances technologiques pour la vidéosurveillance	52
4.	PORTRAIT DU MARCHÉ DE LA SÉCURITÉ ET DE LA VIDÉOSURVEILLANCE .	53
4.1	Marché global de la sécurité	53
4.2	Marché de la vidéosurveillance.....	55
4.2.1	Moteurs du marché de la vidéosurveillance	56
4.2.2	Inhibiteurs du marché de la vidéosurveillance.....	57
4.2.3	Le marché de la vidéosurveillance IP et intelligente.....	57
4.2.4	Les joueurs.....	60
4.2.5	L'impact de la récession sur le marché	60
4.3	L'offre et la demande en vidéosurveillance IP et intelligente au Québec...	62
4.3.1	La demande	62
4.3.2	L'offre	64
4.3.3	Recommandations pour le marché québécois	66

5. ENJEUX	68
5.1 Protection de la vie privée	68
5.2 Efficacité de la vidéosurveillance pour la réduction de la criminalité	70
5.3 Standards pour la vidéo IP	72
BIBLIOGRAPHIE	74
ANNEXE 1 - PROGRAMMES DE RECHERCHE MAJEURS EN VIDÉOSURVEILLANCE INTELLIGENTE	82
ANNEXE 2 - GROUPES DE RECHERCHE (QUÉBEC ET ÉTATS-UNIS)	84
ANNEXE 3 - ENTREPRISES EN VIDÉOSURVEILLANCE (QUÉBEC ET AUTRES).....	86
ANNEXE 4 - ENTREPRISES SPÉCIALISÉES DANS LA CONCEPTION DE LOGICIELS D'ANALYTIQUE VIDÉO	96
ANNEXE 5 - RESSOURCES LIÉES À LA VIDÉOSURVEILLANCE	103

TABLE DES FIGURES

<i>Figure 1 - Caméras de surveillance</i>	<i>15</i>
<i>Figure 2 - Surveillant humain contrôlant plusieurs écrans.</i>	<i>18</i>
<i>Figure 3 - Évolution du matériel de vidéosurveillance</i>	<i>31</i>
<i>Figure 4 - Détection et suivi d'objets.....</i>	<i>38</i>
<i>Figure 5 - Segmentation d'un individu dans une séquence vidéo</i>	<i>40</i>
<i>Figure 6 - Suivi de trajectoires d'objets sur une séquence vidéo.....</i>	<i>42</i>
<i>Figure 7 - Classification d'objets (humains vs véhicules)</i>	<i>42</i>
<i>Figure 8 - Détection d'une plaque d'immatriculation</i>	<i>44</i>
<i>Figure 9 - Tableau tiré du rapport sur les plans et priorités, 2005-2006 à 2008-2009</i>	<i>55</i>

RÉSUMÉ EXÉCUTIF

Remontant à plus de 50 ans, la surveillance au moyen de systèmes de télévision en circuit fermé (TVCF) a connu différents progrès technologiques. Ce rapport de veille technologique et commerciale recense la plus récente avancée dans le domaine, soit le passage à la vidéosurveillance IP intelligente.

L'apparition des premiers enregistreurs numériques, il y a une vingtaine d'années, a amorcé une petite révolution en vidéosurveillance. Depuis, bien qu'il existe encore beaucoup d'équipements analogiques, les réseaux de TVCF intègrent de plus en plus de composantes numériques. De surcroît, la vidéosurveillance migre désormais vers les réseaux informatiques, transmettant la vidéo par protocole IP, sur intranet ou Internet. Quoiqu'encore principalement limitée aux secteurs institutionnels (gouvernements, forces de l'ordre, systèmes de transports, institution d'éducation), la vidéosurveillance IP s'impose comme une tendance irréversible pour l'avenir. Les coûts, ainsi que les configurations informatiques et de réseau qu'elle requiert, freinent, pour l'instant, son adoption chez les plus petits utilisateurs.

Or, caméras de surveillance et images archivées se multiplient. Pour traiter et gérer toute cette vidéo à des fins de sécurité, des logiciels intelligents analysant l'image des caméras ont été développés pour détecter et suivre des objets et signaler des événements suspects. Encore très récente et peu connue, cette technologie, appelée analytique vidéo, offre la promesse d'améliorer la surveillance vidéo. En sécurité physique, le paradigme d'opération passe de plus en plus de l'enquête après le fait à la prévention. L'analytique vidéo pourrait devenir une solution pour détecter les situations suspectes en temps réel, afin d'intervenir sur le champ. Elle permet aussi d'économiser la bande passante en ne transmettant que les données pertinentes pour la surveillance et améliore les capacités de recherche dans les séquences archivées.

À l'heure actuelle, en analytique vidéo, la détection de mouvement, la détection et le suivi d'objets, ainsi que la reconnaissance de visages et de plaques d'immatriculation dans des conditions contrôlées, sont des techniques bien établies. Toutefois, peu de systèmes sont encore suffisamment robustes aux variations et conditions défavorables de l'environnement (changement d'illumination en milieu extérieur, pluie, neige, etc.). La reconnaissance d'objets et d'individus dans des scènes chargées, l'identification d'une personne selon la démarche, la reconnaissance de comportements complexes et l'analytique dans des systèmes à multiples caméras, comptent parmi les principaux défis de la recherche dans ce domaine.

À moyen terme, des facteurs-clés pour le succès de la vidéosurveillance IP intelligente pourraient être 1) la baisse des coûts 2) l'essor des caméras mégapixel utilisant des techniques de compression efficaces (par exemple H.264) et 3) une plus grande disponibilité de caméras intelligentes, avec l'amélioration des traitements analytiques.

Selon différentes études, le marché global de la vidéosurveillance générerait des revenus estimés entre 7,25 milliards de dollars (ÉU) et 14 milliards pour l'année 2007, et qui pourraient croître jusqu'à 46 milliards en 2013. De la même façon, la croissance et les prévisions de croissance dans le sous-secteur de la vidéosurveillance IP sont très robustes. La vidéosurveillance intelligente, quant à elle, constitue une industrie de niche qui en est encore à ses débuts, mais qui est appelée à se développer dans les prochaines années. De nouvelles applications, telles que l'analyse des comportements des consommateurs et la gestion des opérations d'entreprise, pourrait accélérer son essor. Le souci de protéger la vie privée, l'efficacité non démontrée des technologies vidéo pour réduire la criminalité et les efforts en cours pour établir un standard en vidéosurveillance IP sont des facteurs pouvant influencer son utilisation.

Au Québec, la vidéosurveillance est très répandue pour la sécurité et, comme ailleurs, le secteur institutionnel se convertit aux technologies IP et à certaines applications d'analytique. Il existe plusieurs fournisseurs en vidéosurveillance, principalement des distributeurs, installateurs et intégrateurs, mais l'on compte peu de concepteurs de logiciels de gestion vidéo ou d'analytique. L'entreprise québécoise Genetec est un fleuron dans ce domaine. Les produits sur le marché québécois sont essentiellement étrangers.

Le secteur des TI québécois devrait profiter du passage à la vidéosurveillance IP pour développer de nouveaux marchés. Afin de se tailler une place dans l'industrie très concurrentielle de la vidéosurveillance, les entreprises et centres de recherche pourraient prendre le virage intelligent en développant des produits dans le créneau de l'analytique vidéo.



INTRODUCTION

Ce rapport de veille technologique et commerciale vise à dresser un portrait du secteur de la vidéosurveillance intelligente pour la sécurité des gens et des lieux. Il s'agit d'une technologie émergente et encore peu connue qui change le paradigme d'utilisation de la vidéosurveillance traditionnelle et ouvre de nouvelles possibilités. C'est pourquoi elle laisse envisager l'éclosion de nouveaux segments de marchés dans le secteur de la sécurité.

Ce document, destiné à un public non expert, présente les tenants et aboutissants de cette technologie et tente de caractériser le marché qu'elle représente, mondialement, mais aussi, plus particulièrement au Québec. On y collige de l'information sur la technologie de la vidéosurveillance, son application, sa migration vers les réseaux IP, les techniques de pointes en analytique vidéo qui s'y appliquent, les besoins qu'elle suscite, les développements et les tendances dans ce domaine, les enjeux qu'elle soulève, ainsi que l'offre et la demande qu'elle engendre.

Ce rapport résulte d'une recherche documentaire et de la consultation de 14 experts du milieu de la vidéosurveillance et de la sécurité au Québec : chercheurs, développeurs, intégrateurs, installateurs, utilisateurs et bailleurs de fonds. Il se divise en cinq chapitres :

1. Définition du domaine
2. Secteurs d'applications
3. Technologie
4. Portrait du marché de la sécurité et de la vidéosurveillance
5. Enjeux

Aux Annexes 2, 3 et 4, des groupes de recherche en analytique vidéo et des entreprises commercialisant des produits et services en vidéosurveillance IP et intelligente sont répertoriés. Une description de grands programmes de recherche qui ont fait naître le secteur de la vidéosurveillance intelligente, ainsi qu'une liste de ressources en sécurité et vidéosurveillance sont également fournies.

REMERCIEMENTS

Nous remercions vivement les personnes suivantes pour leur précieuse collaboration à ce rapport.

Jean-François Bédard, conseiller en technologies de l'information
Direction de l'innovation et du transfert
Ministère du Développement économique, de l'Innovation et de l'Exportation

René Breyel, président
Claridion

Alain Janelle, président
VideoWave Networks Inc.

Daniel Jeanson, président et directeur aux ventes
SGPTI

Martin Joncas, conseiller en développement industriel
Matériel informatique et instrumentation
Ministère du Développement économique, de l'Innovation et de l'Exportation

Kouame Kouacou, chef de division
Direction principale Métro
Société de transport de Montréal

Frédéric Landry, chef de produit, Applications de surveillance vidéo
ImmerVision

Danielle Lapierre, superviseur, Centre d'appels
Aéroports de Montréal

Denis Laurendeau, Professeur titulaire
Laboratoire de vision et systèmes numériques
Université Laval

Alain Marchildon, vice-président, Applications panoramiques
ImmerVision

Yves Messier, vice-président, Applications de surveillance vidéo
ImmerVision

François Pépin, chef de poste
Sûreté aéroportuaire, Aéroports de Montréal

André Petitclerc, directeur Investissements
Groupe Technologies de l'information et des communications
Société générale de financement du Québec

Jean-Pierre Picard, analyste marketing
Genetec

Ghyslain Proulx, ingénieur de projet en chef TCPE
Société de transport de Montréal

Louis Richer, directeur associé
Service de réseautage et communications
Université McGill

1. DÉFINITION DU DOMAINE

1.1 Sécurité

La sécurité comprend deux aspects : la sécurité physique et la sécurité logique. La sécurité physique *traite des mesures physiques prises pour sauvegarder le personnel, empêcher tout accès non autorisé aux équipements, installations, matériels et documents et à les protéger contre l'espionnage, le sabotage, les détériorations et le vol*¹. Elle couvre donc la protection des personnes, des biens et des lieux.

La sécurité logique cible la protection d'actifs informatiques d'une organisation et vise la mise en vigueur d'un ensemble de mesures de sécurité permettant d'assurer la confidentialité et l'intégrité *des biens informatiques immatériels et des opérations informatiques, et de les protéger contre toute forme de menace accidentelle ou humaine. L'expression biens informatiques immatériels désigne les logiciels, les données et les réseaux*². Avec l'informatisation et la cybercriminalité qu'elle entraîne, la sécurité logique, quoiqu'encore récente, gagne en importance.

Alors que la sécurité physique est habituellement prise en charge par du personnel de sécurité (agents de sécurité, gardiens, services de police, etc.), la sécurité logique relève de spécialistes en technologies de l'information et administrateurs de systèmes informatiques. Toutefois, à l'heure où la protection physique et la surveillance reposent de plus en plus sur des technologies informatiques, sécurité physique et logique ont tendance à converger.

Dans son application, la sécurité peut se répartir en cinq fonctions : protection civile, prévention, intervention, investigation et rétablissement. Depuis les événements du 11 septembre 2001 survenus aux États-Unis, on note un changement de paradigme en sécurité. On vise davantage la prévention d'incidents potentiellement catastrophiques plutôt que l'enquête après le fait. On cherche des méthodes et des technologies qui permettront de détecter les événements suspects et d'en prévenir les dommages sur les personnes, les biens, les lieux et les données.

Au Canada, bien que le sentiment d'insécurité ne soit pas aussi fort qu'aux États-Unis, la lutte contre la criminalité et le renforcement de la sécurité intérieure apparaissent tout de même dans les priorités du gouvernement. Le budget fédéral de février 2008 consacrait 630 millions de dollars sur deux ans à la loi et l'ordre. Le gouvernement accordait aussi 145 millions sur deux ans pour renforcer la sécurité aux frontières. Une série de mesures à cet effet, telles que l'entrée en vigueur du passeport électronique prévue pour 2011 et

¹ Grand dictionnaire terminologique de l'Office de la langue française du Québec.

² Idem.

L'utilisation de biométrie pour délivrer des visas, ont été mises en place. Le gouvernement canadien annonçait également que le budget de la Défense nationale progressera d'un minimum de 1,5 % par année jusqu'en 2010-11.

Le Québec aussi affirme son engagement en matière de sécurité. Dans son plan d'action 2006-2009 découlant de la Politique internationale du Québec, le ministère des Relations internationales du Québec soulève l'importance de contribuer à la sécurité du Québec et du continent nord-américain :

C'est d'abord en protégeant les citoyens sur son territoire, en travaillant à préserver la fluidité des échanges, en sécurisant ses infrastructures stratégiques et en s'assurant qu'il ne devienne une source de menaces pour ses partenaires que le gouvernement du Québec peut le mieux contribuer aux objectifs internationaux de sécurité.³

1.2 Vidéosurveillance

La vidéosurveillance est un segment de l'industrie de la sécurité physique. Cette dernière inclut aussi le contrôle d'accès, la détection et le contrôle d'incendies, la gestion technique de bâtiments, les systèmes assurant la sécurité des personnes et la détection d'intrusion.

La vidéosurveillance consiste à surveiller à distance des lieux publics ou privés, à l'aide de caméras, le plus souvent motorisées, qui transmettent les images saisies à un équipement de contrôle qui les enregistre ou les reproduit sur un écran (Figure 1)⁴. Elle capte sur image les flux de personnes pour surveiller les allées et venues, prévenir les vols, agressions et fraudes, ainsi que pour gérer les incidents et mouvements de foule.⁵



Figure 1 - Caméras de surveillance

³ Ministère des Relations internationales du Québec,
http://www.mri.gouv.qc.ca/fr/politique_internationale/securite/index.asp.

⁴ Grand dictionnaire terminologique de l'Office de la langue française du Québec.

⁵ <http://fr.wikipedia.org/wiki/Videosurveillance>.

Bien que ses premières utilisations remontent aux années 1950, la surveillance au moyen de systèmes de télévision en circuit fermé (TVCF) s'est vraiment développée à partir des années 1970, principalement au Royaume-Uni, pour lutter contre les activités terroristes. À l'heure actuelle, le Royaume-Uni constitue d'ailleurs la société « la plus surveillée » avec un nombre estimé à plus de quatre millions de caméras de surveillance déployées sur son territoire. L'implantation de la vidéosurveillance s'est intensifiée au cours des années 1990, mais elle a connu un développement fulgurant suite aux attentats de septembre 2001 aux États-Unis, et puis ceux de Londres en 2005.

La peur grandissante face au terrorisme n'est pas le seul facteur d'adoption de la technologie de vidéosurveillance. Celle-ci s'avère indispensable pour le suivi des opérations et la gestion des incidents de sécurité dans les lieux publics et privés. De plus, elle constitue un outil d'enquête irremplaçable pour la résolution de crimes, de méfaits ou de litiges. Toutefois, la preuve ne semble pas encore faite que la vidéosurveillance actuelle permette de prévenir les incidents de sécurité ou qu'elle fasse chuter la criminalité.

Un réseau de télévision en circuit fermé (TVCF)⁶ est un système vidéo qui transmet des images en boucle fermée. Autrefois uniquement analogiques, les réseaux TVCF intègrent maintenant des composantes numériques. L'accès au réseau de transmission peut, dans certains cas, se faire par Internet. Seuls des utilisateurs détenant des droits d'accès au réseau peuvent accéder à l'information fournie par les caméras.

Les activités de sécurité d'un réseau de TVCF sont⁷ :

- Dissuasion
- Observation
- Surveillance
- Collecte de renseignements
- Évaluation d'un incident probable et intervention connexe
- Évaluation d'un incident en cours et intervention connexe
- Analyse judiciaire après l'incident
- Analyse des éléments de preuve après l'incident

Il existe trois types de vidéosurveillance :

- Active : surveillance d'une aire pour appuyer le travail sur place d'agents de sécurité ou lors d'intervention d'urgence.
- Passive : un employé surveille un petit nombre d'écrans de télévision en s'adonnant à d'autres tâches.

⁶ CCTV en anglais.

⁷ Tiré de [2].

- Enregistrement : permet de collecter des renseignements, à des fins d'enquête et de preuve. Les enregistrements sont conservés pendant une durée déterminée, dépendant des besoins et des limites des espaces d'archivages.

1.3 Vidéosurveillance intelligente

L'analytique vidéo (video analytics⁸), aussi appelée vidéosurveillance intelligente, est une technologie qui permet, au moyen de logiciels, d'identifier automatiquement, dans des séquences vidéo, des objets, des comportements ou des attitudes spécifiques. Elle transforme la vidéo en données qui seront transmises ou archivées pour permettre au système de vidéosurveillance d'agir en conséquence. Il pourra s'agir d'actionner une caméra mobile, dans le but d'obtenir des données plus précises de la scène ou, tout simplement, d'envoyer une alerte au personnel de surveillance pour qu'il puisse prendre une décision sur l'intervention adéquate à apporter.

Les systèmes de vidéosurveillance intelligente utilisent des algorithmes mathématiques pour détecter des objets en mouvements dans l'image et filtrer les mouvements non pertinents. Ils créent une base de données consignnant les attributs de tous les objets détectés et leurs propriétés de mouvements. La prise de décision par le système ou la recherche d'événements d'intérêt dans des séquences archivées se fait à partir de règles (par ex.: si une personne traverse une limite, envoyer une alerte).

1.3.1 Raisons pour l'utilisation de vidéosurveillance intelligente

De nos jours, les réseaux de vidéosurveillance comptent un plus grand nombre de caméras. Pour de grandes infrastructures, par exemple un réseau de transport en commun, plus de mille caméras de surveillance peuvent être déployées. Ces installations représentent une quantité colossale de vidéo à transmettre, visionner et archiver. Il devient donc impossible pour un surveillant humain d'analyser toute cette vidéo, afin d'y déceler les comportements ou événements suspects. D'autant plus que le personnel des centres de surveillance doit gérer d'autres tâches, telles que le contrôle d'accès, l'émission des badges/clés/permis, le traitement des appels d'urgence, le suivi des alarmes d'incendie, le contrôle des communications radio.

Plusieurs études démontrent les limites de la surveillance humaine (Figure 2). Après seulement 20 minutes à regarder et analyser des écrans de surveillance vidéo, l'attention de

⁸ En anglais, le terme *video analytics* est utilisé pour référer à l'analyse vidéo faite spécifiquement pour la vidéosurveillance. En français, il ne semble pas y avoir de terme consacré pour ce domaine, certains utilisant « analytique vidéo » et d'autres « analyse vidéo ». Pour ce rapport, nous avons opté pour le néologisme « analytique vidéo ». Les termes *Intelligent video surveillance* ou *smart video surveillance* sont aussi utilisés en anglais pour décrire cette technologie.

la plupart des individus chute sous un niveau acceptable⁹. Un surveillant ne peut suivre attentivement 9 à 12 caméras plus de 15 minutes¹⁰. Or, certaines études rapportent que le rapport entre le nombre d'écrans et le nombre de caméras peut se situer entre 1 :4 et 1 :78 dans certains réseaux de vidéosurveillance¹¹. On estime à 1 sur 1 000 la probabilité de réagir sur le fait à un événement capté par un réseau de caméras de surveillance¹². C'est pourquoi, historiquement, la vidéosurveillance constitue principalement un outil d'enquête après l'événement.



Figure 2 - Surveillant humain contrôlant plusieurs écrans.

Dans ce contexte, l'analytique vidéo présente de nombreux avantages :

- Elle est en fonction 24 heures par jours, sept jours par semaine.
- Elle peut enclencher une alarme qui sera traitée par un opérateur humain ou commander le déplacement ou zoom d'une caméra pour une surveillance plus précise de l'événement, permettant ainsi une intervention en temps réel, plutôt qu'après l'événement.
- Elle réduit la bande passante et l'espace d'archivage nécessaires en ne transmettant ou n'enregistrant que les données sur les événements pertinents.
- Elle libère le personnel de sécurité d'une surveillance continue.
- Elle permet la recherche rapide d'événements pertinents dans les séquences vidéo archivées.
- Elle permet d'identifier les objets dans une scène et de suivre leur activité (*situation awareness*).

⁹ Étude du US National Institute of Justice, cité dans [5].

¹⁰ ASIS International, cité dans [5].

¹¹ Étude de l'Université Kingston citée dans [8].

¹² CCTV Today (nov 2005), tiré de [5].

Néanmoins, il s'agit d'une technologie encore récente, qui comporte de nombreuses limites techniques. Par exemple, la discrimination entre les comportements usuels et suspects est un problème difficile à traiter pour une machine. Comment discerner si une personne court parce qu'elle est en retard ou parce qu'elle vient de commettre un délit ?

En intelligence artificielle, il existe toujours un compromis entre le taux de reconnaissance obtenu et le nombre de fausses alarmes. Dans le cas des systèmes intelligents de surveillance, plus le seuil de détection sera permissif, meilleures seront les chances de détecter une menace de sécurité réelle, mais plus nombreuses seront les alarmes sonnées inutilement. Puisque chaque alarme doit être évaluée par un surveillant, il est primordial de maintenir le taux de fausses alarmes bas, pour éviter les pertes de temps et de productivité du personnel de surveillance. Ceci constitue un défi de performance de taille lorsque vient le temps de commercialiser une technologie d'analytique vidéo.

1.3.2 Facteurs déterminant le choix d'un système de vidéosurveillance intelligente

- Taux de reconnaissance / fausses alarmes visées.
- Pourcentage des caméras dont les images seront analysées par ordinateur.
- Nature de la scène à surveiller : l'analytique vidéo est plus appropriée pour les scènes présentant peu de changements, ennuyantes pour une surveillance humaine (risque d'inattention), tandis qu'un surveillant humain surpasse la machine pour les scènes très actives présentant beaucoup d'occlusions.
- Extensibilité : possibilité d'ajouter des caméras supervisées par ordinateur ou d'augmenter leur pourcentage dans le réseau.

2. SECTEURS D'APPLICATIONS

À son origine, la vidéosurveillance a d'abord été utilisée par les services publics (police, transports, administrations). Elle fut ensuite adoptée par des entreprises désirant protéger des actifs stratégiques, telles que les raffineries, les centrales nucléaires, les barrages fluviaux, les usines agroalimentaires et les complexes pharmaceutiques. Les casinos apparaissent aussi comme des précurseurs dans le déploiement de grands systèmes de vidéosurveillance. De nos jours, les caméras de surveillance sont présentes dans divers lieux publics et privés : immeubles, commerces, stationnements, gares, aéroports, routes, transports publics, banques, etc.

Les systèmes de vidéosurveillance sont déployés à différentes échelles. Pour la surveillance de crimes mineurs (par ex., attaques, vandalisme, vols), la vidéosurveillance est principalement utilisée pour l'enquête après le fait. Ce niveau de surveillance requiert des technologies simples, le plus souvent analogiques, qui n'intègrent pas d'intelligence vidéo. C'est le type de système qu'on peut retrouver au dépanneur du coin, dans un petit commerce ou dans une résidence privée.

La surveillance d'immeubles ou de commerces de plus grande taille nécessite souvent un réseau plus étendu de caméras. La surveillance vise principalement le contrôle des voies d'accès, des stationnements et, s'il s'agit de magasins, des rayons et points de vente. La vidéosurveillance y est surtout utilisée pour les fins d'enquête. Cependant, ces usagers souhaiteraient obtenir des systèmes de surveillance capables de générer des alertes en temps réel pour permettre une intervention immédiate. Les produits d'analytiques vidéo accomplissent donc une percée dans ces secteurs. Le retour sur l'investissement constitue un facteur déterminant pour l'achat d'équipements de vidéosurveillance intelligente pour cette clientèle.

La vidéosurveillance à grande échelle se retrouve dans les villes et les quartiers, les systèmes de transport, les campus académiques, les grands événements (festivals, sommets économiques, jeux olympiques, etc.), les périmètres de sécurité étendus. Elle nécessite le déploiement de plusieurs dizaines, voire de centaines de caméras. Celles-ci doivent parfois être accessibles à des centaines d'intervenants en sécurité, provenant de différentes agences gouvernementales, corps policiers ou services d'urgence. Dans ces installations, la vidéosurveillance s'ajoute à une panoplie de systèmes de sécurité et de contrôle : contrôle d'accès, d'incendie, téléphonie, communications radio, systèmes géomatiques, etc. Étant donné le nombre de caméras vidéo impliquées et l'importance des interventions d'urgence, ces applications sont particulièrement propices à l'utilisation d'analytique vidéo pour le traitement automatisé des flux vidéo générant des alarmes lors d'événements suspects. Comme les budgets alloués aux systèmes de surveillance dans ces infrastructures sont souvent importants, l'ajout de logiciels d'analytique peut plus facilement y être envisagé.

Il faut noter une utilisation assez récente de la vidéosurveillance dans des unités mobiles : voitures de patrouille, ambulances, autobus, etc. La transmission sans fil des signaux vidéo à un centre de surveillance peut poser problème.

2.1 Gouvernement et sécurité publique

Les différents paliers de gouvernement doivent assurer la sécurité de la population, ainsi que des infrastructures publiques. Au niveau national, elle sera utilisée, par exemple, pour surveiller les éléments suivants :

- Infrastructures sensibles
- Frontières
- Édifices et sites gouvernementaux
- Laboratoires
- Bases militaires
- Prisons

À un niveau local, la vidéosurveillance est implantée dans plusieurs villes dans le monde pour surveiller la criminalité et servir d'outil pour les interventions d'urgence. Elle contribue aussi à assurer la sécurité lors de grands rassemblements (spectacles, manifestations, événements sportifs). Londres est la ville la plus souvent citée pour le nombre de caméras déployées dans ses rues. La surveillance vidéo sert aussi à gérer le stationnement, notamment pour le contrôle des permis de stationnement, l'application des règles, la détection des vols, vandalismes ou méfaits, et le contrôle d'accès.

La vidéosurveillance est abondamment utilisée par les forces de l'ordre pour mener les enquêtes, surveiller les personnes et les véhicules recherchés, détecter les activités dangereuses ou criminelles. On la retrouve aussi à bord des autos-patrouilles pour la vérification des interventions policières.

On retrouve de plus en plus de caméras le long des tronçons routiers pour surveiller la circulation et détecter les incidents, les comportements dangereux ou les infractions. Montréal possède un réseau de plusieurs caméras et des stations de détection de véhicules permettant le suivi en temps réel des conditions de la circulation et la détection automatique des incidents¹³.

Le secteur gouvernemental présente plusieurs besoins pour la vidéosurveillance intelligente : identification d'individus et de véhicules, comptage de personnes et surveillance de foules, reconnaissance de comportements suspects ou violents (bagarres, méfaits), détection d'intrusions, monitoring routier. Des analyses plus poussées, telles que la reconnaissance d'émotions par ordinateur ou du mensonge chez un individu, sont aussi envisagées.

2.2 Éducation

La vidéosurveillance est de plus en plus présente dans les établissements scolaires. Son utilisation vise à assurer la sécurité des enseignants et étudiants, ainsi que la protection des actifs contre le vandalisme et le vol. Les tueries tragiques survenues en milieu scolaire, tels qu'à l'école Columbine, aux États-Unis, et ici au Québec, à l'école Polytechnique et au Collège Dawson, ont fait ressortir l'importance de surveiller plus adéquatement les campus scolaires. Ceux-ci, particulièrement dans le cas des universités, peuvent être étendus et posséder plusieurs bâtiments, de nombreux accès à contrôler et des stationnements à surveiller. Dans ce milieu, la vidéosurveillance sert notamment à :

- surveiller l'accès au périmètre de l'établissement, parfois étendu, dans le cas d'un campus universitaire ;
- surveiller le matériel, les équipements et les données ;

¹³ Transports Québec, http://www.mtg.gouv.qc.ca/portal/page/portal/regions/montreal_ile/gestion_circulation.

- détecter et suivre les actes de vandalisme, vols, méfaits, comportements inappropriés ;
- reconnaître les plaques d'immatriculation ;
- supporter les enquêtes criminelles ;
- contrôler les accès.

Comme les établissements d'éducation possèdent souvent une infrastructure réseau IP, il peut s'avérer avantageux pour eux d'y déployer des systèmes de vidéosurveillance numériques.

2.3 Commerce de détail

Le commerce de détail représente un marché en expansion pour la vidéosurveillance. Celle-ci y est utilisée autant pour des aspects de sécurité intérieure (magasin, entrepôt) qu'extérieure (stationnement). Même les plus petits commerces se dotent de caméras pour, minimalement, conserver des preuves vidéo en cas de vols ou d'incidents. Dans les chaînes de magasins, des systèmes de vidéosurveillance beaucoup plus sophistiqués sont déployés pour permettre la surveillance centralisée des différentes succursales. Dans l'ensemble du secteur, la vidéosurveillance visera notamment :

- la surveillance des caisses et des transactions (vols, fraudes par les employés) ;
- la protection des biens matériels et des infrastructures ;
- la surveillance de l'inventaire, des marchandises (livraisons) ;
- la protection du personnel et des clients ;
- le contrôle d'accès aux aires verrouillées ;
- la vérification des situations d'urgence (incendie, alarmes, etc.) ;
- la surveillance des stationnements, des véhicules, des entrées et sorties.

Considérant les risques élevés de vols et d'attaques auxquels sont exposés les commerces de détail, ainsi que les pertes importantes qui en découlent, la vidéosurveillance s'impose comme un outil incontournable pour assurer la sécurité des employés et de la marchandise. De plus, il existe dans ce marché un potentiel réel pour l'analytique vidéo. Par exemple, on retrouve des systèmes qui combinent l'information vidéo et les données de la caisse, afin de vérifier que les articles sortis par les clients ont effectivement été facturés. Cette technologie permet, par exemple, de prévenir les fraudes aux points de vente impliquant la complicité des caissiers.

De plus, la vidéosurveillance intelligente est de plus en plus utilisée à des fins qui dépassent la sécurité, comme la gestion des opérations et la mise en marché. Dans ce contexte, l'analytique vidéo servira, notamment, à compter les clients, à analyser leurs comportements et déplacements en magasin et à compiler des statistiques sur les habitudes de consommation. Par exemple, ici au Québec, la firme québécoise Organix IT a équipé la

chaîne des dépanneurs Couche-Tard d'un système de vidéosurveillance intelligente offrant ces possibilités¹⁴.

2.4 Transports

La sécurité et le bon fonctionnement des aéroports, des gares, des ports et des transports publics est critique pour l'économie d'un pays. Un incident de sécurité peut gravement perturber leurs opérations et se traduire en pertes significatives. Or, étant donné les flots importants de passagers qui y transitent et l'étendue de leurs infrastructures, les systèmes de transports font face à des défis de sécurité hors du commun. Les actes terroristes commis dans différents systèmes de transports dans le monde ont exacerbé ces défis.

Les logiciels d'analytique ciblent le secteur des transports en offrant différentes fonctions adaptées : détection d'intrusion dans un périmètre ou une zone contrôlée, détection de personnes pénétrant dans une voie de sortie, détection de bagage abandonné, reconnaissance de visages, comptage de personnes, reconnaissance de plaques d'immatriculation pour le contrôle d'accès aux stationnements, détection de comportements suspects (rôdeurs, vandalisme, graffiti), détection de personnes sur les voies. Toutefois, le milieu des transports représente de grands défis techniques pour les systèmes de vidéosurveillance intelligente, considérant le nombre des personnes qui passent dans le champ de la caméra, la diversité des comportements des passagers et les conditions défavorables pour les caméras (vibrations, poussière, etc.). De plus, pour la surveillance extérieure, les caméras et algorithmes analytiques doivent pouvoir fonctionner en dépit des variations météorologiques (brume, neige, pluie, etc.).

2.4.1 Aéroports

Après les événements du 11 septembre 2001, les mesures de sécurité ont connu un resserrement, particulièrement dans les grands aéroports, et de nouvelles technologies ont été déployées. Pour les aéroports, la priorité consiste à contrôler l'accès aux zones sécurisées, principalement l'accès aux avions, mais aussi à assurer la sécurité des passagers, du personnel et des biens sur l'ensemble du périmètre (pistes, stationnements, voies d'accès, etc.).

Selon les recherches faites pour ce rapport, la vidéosurveillance intelligente semble encore peu adoptée dans les aéroports canadiens. Par exemple, à l'aéroport Pierre-Elliott Trudeau de Montréal, la vidéosurveillance est surtout utilisée pour assister les interventions d'urgence. Lorsqu'un incident est signalé, une caméra mobile pivote pour suivre les opérations en direct, à partir d'un centre de surveillance. Le contrôle d'accès repose

¹⁴ Intelligent Security Systems, <http://www.isscctv.com/company/publicity/1645/>.

principalement sur des technologies biométriques d'identification (empreintes, iris), l'utilisation de cartes à puces et de NIP¹⁵. La vidéo de surveillance est archivée et sert également comme élément de preuve pour les enquêtes des corps policiers. Elle se retrouve aussi à bord des véhicules de patrouille. Pour le moment, les caméras sont majoritairement analogiques et peu d'analytique vidéo est utilisée. Parmi les fonctions intelligentes déjà en place, on retrouve le comptage de personnes pour évaluer, par exemple, les temps de traitement à la douane, ainsi que la reconnaissance de plaques d'immatriculation qui permet de recenser les voitures dans les stationnements et de détecter des vols. Aéroports de Montréal devrait prochainement ajouter une nouvelle partie à son système de vidéosurveillance qui sera entièrement IP et devrait inclure caméras intelligentes et logiciels de traitement vidéo.

2.4.2 Gares et transports publics

Pour les gares et les transports publics, la vidéosurveillance vise surtout la surveillance des voix d'accès, des quais, des rails et tunnels, des stationnements et de toutes les structures auxiliaires permettant d'assurer le service. Elle s'allie à d'autres systèmes de contrôle d'accès et dispositifs de sécurité pour assurer la protection des passagers, du personnel et des infrastructures. La vidéo est visionnée en direct à partir du centre de surveillance, ou en différé pour les enquêtes suite à des incidents de sécurité.

Au Québec, la Société de transport de Montréal (STM) poursuit le déploiement de plus de 1 600 caméras dans les infrastructures du métro de Montréal, grâce à la contribution des deux paliers de gouvernement, afin d'augmenter la sécurité de ses usagers. Des caméras font aussi leur apparition dans certains autobus du réseau, à titre de prototype. La Société de transport de Laval équipera aussi une partie de ses autobus avec des caméras de surveillance pour contrer le vandalisme¹⁶. Le nouveau système du métro, complètement sur réseau IP, représente l'un des projets phare en matière de vidéosurveillance IP au Québec. Doté d'une commande centralisée, la vidéosurveillance s'intègre avec les différents systèmes de contrôle et de maintenance. La STM commence à déployer de l'analytique vidéo pour la détection automatisée de personnes sur les voies. La société de transport se dit dans les premières au Canada à exploiter la vidéo intelligente dans les transports en commun. En cette matière, les systèmes de transports publics canadiens accusent un retard sur ceux de pays européens, tels que le Royaume-Uni, la France et l'Allemagne qui sont beaucoup mieux équipés en vidéosurveillance. À long terme, si l'usage de l'analytique vidéo s'avère efficace, la STM envisage certaines autres applications, telles que la détection de colis suspects, la surveillance des portes et la reconnaissance de comportements suspects.

¹⁵ Numéro d'identification personnel.

¹⁶ Morissette, H., *Des caméras seront installées dans les autobus de Laval*, 24 heures, 3 décembre 2008, p. 6.

2.4.3 Ports

Comme pour les autres systèmes de transports, dans les ports, la vidéosurveillance intelligente est utilisée pour la protection des passagers et du personnel, pour la surveillance des allées et venues dans le périmètre et pour l'identification de véhicules dans ce périmètre. Toutefois, les ports présentent des défis particuliers pour l'analytique vidéo, parce qu'ils requièrent la surveillance des eaux avoisinantes. Les reflets sur l'eau, ainsi que le mouvement des vagues constituent des variations environnementales pouvant perturber les algorithmes analytiques, notamment pour la détection de mouvement.

2.5 Milieu bancaire

La vidéosurveillance est très utilisée pour assurer la sécurité des banques. Dans un premier temps, la présence de caméras opère un certain pouvoir de dissuasion sur la perpétration de vols à mains armées et d'agressions. Si un tel délit survient, les séquences vidéo archivées servent à l'enquête et l'identification des malfaiteurs.

Les guichets automatiques sont particulièrement à risque pour les actes criminels. Les caméras de surveillance aident à détecter les fraudes, comme par exemple, l'installation d'un dispositif pour lire l'information magnétique des cartes de guichet.

Pour le milieu bancaire, la vidéosurveillance intelligente peut augmenter l'efficacité de la surveillance. Elle permet d'assurer un suivi sur l'ensemble du réseau des succursales, afin d'y détecter les individus ou comportements suspects. Elle permettra, entre autres, de retrouver toutes les séquences vidéo provenant de toutes les succursales où apparaît un certain individu, grâce à des techniques de reconnaissance faciales.

2.6 Industrie du jeu et casinos

Les casinos et centres de jeux ont recours depuis longtemps à la vidéosurveillance pour protéger les clients et les lieux, mais aussi pour détecter la triche, les coups montés, les vols à la caisse et autres méfaits pouvant occasionner des pertes. Elle sera aussi utilisée à titre de preuve pour évaluer la validité de poursuites en dommages et intérêts intentées contre l'institution de jeu.

Comme la surveillance d'un casino exige de suivre les comportements de plusieurs personnes dans un environnement chargé, la vidéosurveillance intelligente offre une avenue intéressante pour assister le personnel de sécurité dans leur tâche. La détection et la reconnaissance de visages et de gestes font partie des fonctionnalités analytiques utiles pour ce milieu.

2.7 Autres

La vidéosurveillance est déployée dans beaucoup d'autres milieux. On la retrouve dans les commerces et pour la surveillance d'édifices. Elle sert, le plus souvent, à filmer les voies d'accès et les stationnements, à surveiller les valeurs matérielles et à assurer la protection des employés et des clients.

La surveillance vidéo trouve aussi sa place en santé pour assister les interventions. On peut même la retrouver à bord des ambulances, en combinaison avec d'autres instruments de mesure, pour permettre le suivi du patient à distance. L'entreprise américaine IndigoVision a développé des solutions d'analytiques embarquées dans des caméras intelligentes spécifiquement pour détecter le mouvement des hélicoptères qui atterrissent sur le site d'un hôpital américain.

Le marché grand public se développe aussi. De plus en plus de systèmes de vidéosurveillance pour les résidences sont en vente, même dans les magasins non spécialisés. Les caméras complètent maintenant les différents dispositifs de surveillance et de sécurité pour le secteur résidentiel.

3. TECHNOLOGIE

3.1 Architecture des systèmes de vidéosurveillance

3.1.1 Composantes d'un système de vidéosurveillance

Cette section présente, de façon sommaire, les différentes composantes matérielles et logicielles des systèmes de vidéosurveillance. Une description plus détaillée de l'infrastructure des systèmes de vidéosurveillance, ainsi que des principes guidant les choix matériels, peut être retrouvée dans de nombreux ouvrages et guides de références, incluant [1] et [20].

3.1.1.1 Acquisition

Il existe une panoplie de modèles de caméras répondant à différents besoins de surveillance. Elles sont analogiques ou numériques et peuvent être motorisées ou non. Plus spécifiquement, on retrouve les types de caméras suivants.

- **Fixe** : Pointée dans une direction unique, elle couvre une zone définie (une entrée, une portion de stationnement, etc.). C'est la caméra de surveillance traditionnelle. Elle constitue un excellent choix lorsqu'on désire que la présence de la caméra, ainsi que sa direction de surveillance, soient visibles.

- **PTZ (Pan-Tilt-Zoom)** : Motorisée, elle peut être actionnée, manuellement ou automatiquement, dans des mouvements panoramique/inclinaison/zoom. Elle sert à suivre des objets ou des individus se déplaçant dans la scène ou à zoomer sur des régions d'intérêt (par exemple, sur une plaque d'immatriculation).
- **Dôme** : Recouverte d'un caisson hémisphérique, ce qui la rend discrète et, dans certains modèles, résistante au vandalisme et aux intempéries. Elle peut être fixe ou mobile. Les versions motorisées couvrent une zone très large, grâce à leur balayage horizontal de 360° et de 180° à la verticale. Bien qu'en « tour de garde », elle puisse remplacer dix caméras fixes en balayant l'aire à surveiller, elle n'observe qu'une seule direction à la fois.
- **Mégapixel** : Offre une résolution plus élevée que les caméras standards, allant de 1 à 16 mégapixels¹⁷. Elle permet soit de capter une image plus détaillée, soit de couvrir un plus large champ visuel, réduisant le nombre de caméras nécessaires pour couvrir une aire à surveiller. Lorsqu'utilisée avec un grand angle, elle possède un espace de visualisation allant généralement de 140° à 360°. Offrant la possibilité de zoomer de façon logicielle dans l'image, elle peut ainsi devenir une alternative à la caméra PTZ mécanique qui entraîne l'usure des pièces. Sa résolution élevée contribue à l'amélioration de la performance des algorithmes de détection et de reconnaissance exigeant un haut niveau de détails, telles que la lecture de plaques d'immatriculation et la reconnaissance de visage.
- **Infrarouge et thermique** : Sensible au rayonnement infrarouge (IR), elle est capable de produire une image de bonne qualité dans le noir pour une surveillance nocturne. De nuit, elle filme en noir et blanc, mais elle peut produire une image couleur le jour. Certaines caméras infrarouges sont équipées de leur propre source de lumière IR, allumée lorsque le niveau d'éclairage chute sous un certain seuil. Des projecteurs IR séparés (lampe ou LED¹⁸) peuvent aussi être utilisés. Les caméras thermiques enregistrent le rayonnement de chaleur des objets. Elles ne requièrent aucune source d'illumination.
- **Panoramique** : Grâce à une optique spéciale, elle offre 360° de visibilité avec une seule caméra¹⁹. Elle permet un PTZ virtuel dans l'image. Les principales technologies panoramiques pour la surveillance sont le fisheye, la lentille à miroirs et la lentille panomorphe. Toutefois, la résolution de ces caméras est souvent insuffisante pour des analyses nécessitant un niveau de détail élevé.

3.1.1.2 Transmission

La vidéo captée par les caméras de surveillance doit être transmise aux systèmes d'enregistrement, de traitement et de visionnement. Cette transmission peut se faire par

¹⁷ En 2008, ne représentait que 4 % des caméras vendues, mais leurs ventes progressent rapidement.

¹⁸ *Ligth Emitting Diodes*.

¹⁹ ImmerVision et Grandeye développent deux technologies majeures de surveillance panoramique.

câble (câbles coaxiaux ou à fibre optique, fils de cuivre torsadés) ou à travers l'air (signaux infrarouges, transmission radioélectrique).

La **vidéo filaire** prédomine largement dans les systèmes de vidéosurveillance. Elle offre une plus grande bande passante et une meilleure fiabilité que les connections sans fil, à un coût inférieur. Cependant, la **transmission vidéo sans fil** s'impose parfois comme solution, par exemple dans le cas de surveillance de grands périmètres où l'installation de câblage s'avérerait trop coûteuse, ou lorsque les zones à surveiller sont impossibles à rejoindre par câble.

Qu'il transite par fil ou sans fil, le signal vidéo peut être analogique ou numérique. Encore aujourd'hui, la majeure partie des transmissions vidéo pour la surveillance sont **analogiques**. Néanmoins, les réseaux informatiques (LAN, WAN ou Internet) sont de plus en plus utilisés pour transporter la vidéo grâce au **protocole IP**. Les caméras IP peuvent se connecter directement sur ces réseaux, tandis que les flux vidéo émergeant de caméras analogiques doivent, au préalable, être numérisés par un **encodeur**, aussi appelé **serveur vidéo**, pour passer par les réseaux IP.

3.1.1.3 Compression

La vidéo numérisée représente une grande quantité de données à transmettre et à archiver. L'envoi d'une séquence vidéo peut nécessiter jusqu'à 165 mégabits de bande passante et la vidéo d'une seule caméra pour une journée peut occuper sept gigaoctets d'espace disque. C'est pourquoi la vidéo de surveillance doit être compressée grâce à des **codecs**²⁰, algorithmes permettant de réduire la quantité de données en supprimant les redondances, par image ou entre les trames d'une séquence, ainsi que les détails imperceptibles à l'œil humain.

Selon le type de compression, l'usage du processeur requis pour l'exécution du codec est plus ou moins intensif. Un compromis s'impose donc entre le taux de compression et les ressources du processeur qui sont accaparées.

Il existe deux grands groupes de standards internationaux de compression : JPEG, créés par le Joint Photographic Experts Group, et MPEG, élaborés par le Moving Photographic Experts Group. Dans le premier groupe, on retrouve les formats JPEG pour les images fixes, et MJPEG pour les séquences vidéo. Le second groupe comprend les formats MPEG-1, MPEG-2, MPEG-4 et H.264²¹.

À l'heure actuelle, MJPEG et MPEG-4 sont les standards les plus répandus en vidéosurveillance. Toutefois, avec les améliorations en qualité et efficacité (taux de compression, latence, résistance à l'erreur) qu'il apporte, H.264 devrait bientôt remplacer

²⁰ Contraction de Codeur-décodeur.

²¹ Appellation commune de MPEG-4 Part 10 AVC/H.264.

MPEG-4. En effet, sans affecter la qualité de l'image, l'encodeur H.264 permet de réduire la taille de celle-ci de plus de 80 % par rapport à la compression MJPEG, et de 50 % par rapport à la compression MPEG-4 [15].

3.1.1.4 Traitement

Les systèmes de gestion vidéo opèrent les traitements des images de vidéosurveillance, tels que la gestion des différents flux vidéo, le visionnement, l'enregistrement, l'analyse et la recherche dans les séquences enregistrées. Il existe quatre grandes catégories de systèmes de gestion vidéo.

- **Enregistreur vidéo numérique (DVR²²)** : Appareil qui dispose d'un disque dur interne pour l'enregistrement numérique de la vidéo et d'un logiciel intégré de traitement de la vidéo. Il n'accepte que les flux provenant de caméras analogiques, qu'il numérise. Les modèles récents permettent de visionner la vidéo à distance sur ordinateur. Encore très répandus, ils laissent toutefois peu à peu leur place aux systèmes supportant la vidéo IP de bout en bout.
- **Enregistreur vidéo hybride (HDVR²³)** : Similaire à l'enregistreur numérique, mais accepte à la fois le branchement de caméras analogiques et IP. Il est possible de rendre hybrides plusieurs modèles d'enregistreurs vidéo numériques par l'ajout d'un logiciel.
- **Enregistreur numérique réseau (NVR²⁴)** : Conçu pour les architectures réseaux IP de vidéosurveillance, il ne peut traiter que les signaux vidéo provenant de caméras IP ou d'encodeurs.
- **Logiciel de vidéosurveillance IP** : Solution purement logicielle de gestion de la vidéo sur un réseau IP. Dans le cas de systèmes de surveillance comportant peu de caméras, un navigateur Web peut suffire à gérer la vidéo. Pour de plus gros réseaux de vidéosurveillance, un logiciel dédié de gestion vidéo doit être utilisé. Celui-ci s'installe sur un ordinateur personnel ou un serveur. Plus complexe à installer, en raison des configurations nécessaires du serveur, il offre une plus grande flexibilité pour le choix et l'ajout de composantes au réseau de vidéosurveillance. Les logiciels de vidéosurveillance IP représentent une tendance forte en gestion vidéo, surtout dans les infrastructures comportant un grand nombre de caméras. Les plateformes ouvertes permettent d'intégrer facilement des caméras et composantes matérielles de différents fabricants.

3.1.1.5 Archivage

La période d'archivage des séquences vidéo varie selon les besoins de surveillance, allant de quelques jours à quelques années. En moyenne, les organisations conservent les preuves vidéo entre 30 et 90 jours. Le déploiement de vastes réseaux de caméras et l'utilisation de

²² Digital Video Recorder.

²³ Hybrid Digital Video Recorder.

²⁴ Network Video Recorder.

vidéosurveillance à haute résolution fait exploser les demandes pour les systèmes de stockage. Bien que le coût des supports d'enregistrement ait considérablement baissé dans les dernières années, l'archivage représente souvent une part importante des dépenses d'infrastructure en vidéosurveillance, en raison de la quantité toujours croissante de données vidéo à stocker.

Les solutions de stockage sont de deux types :

- **Interne** : Les disques durs intégrés aux enregistreurs vidéo numériques ou aux serveurs représentent la forme d'archivage la plus répandue. Elle peut offrir jusqu'à quatre téraoctets d'espace. Certaines caméras IP disposent même d'une carte mémoire ou d'un disque USB permettant d'enregistrer des heures, voir des jours de vidéo. Les solutions internes d'archivage conviennent bien pour les systèmes de vidéosurveillance de taille modeste, comprenant jusqu'à 50 caméras.
- **Rattaché** : L'archivage se fait sur des appareils externes aux enregistreurs ou serveurs vidéo. De type NAS (*Network Attached Storage*) ou SAN (*Storage Area Network*), ces systèmes offrent un espace de stockage partagé entre les différents clients du réseau. Sur un système de stockage en réseau NAS, un fichier est archivé sur un même disque dur, alors qu'avec le réseau de stockage SAN, un fichier peut être sauvegardé en fragments répartis sur plusieurs supports de stockage. Ces solutions d'archivage rattachées sont particulièrement avantageuses pour les grands réseaux de vidéosurveillance comportant un grand nombre de caméras²⁵. Bien que plus onéreuses que les systèmes internes d'archivage, ces solutions rattachées sont supérieures en termes d'extensibilité, de flexibilité et de redondance.

3.1.1.6 Affichage

Une grande partie de la vidéo captée par les caméras de surveillance n'est jamais regardée. Elle est simplement archivée, au cas où un visionnement soit nécessaire suite à un incident. Traditionnellement, la vidéosurveillance a principalement servi comme outil d'enquête. Toutefois, dans plusieurs cas de surveillance, des agents de sécurité visionnent, en temps réel, les images provenant des caméras de surveillance. Sans nécessairement regarder toute la vidéo captée, les agents peuvent faire une revue périodique des différentes sources vidéo.

La vidéo de surveillance peut être visionnée sur différents appareils. Dans de petites installations, il est possible de regarder la vidéo directement de l'enregistreur, simultanément à son enregistrement. Plus généralement, les images seront regardées à distance, sur un ordinateur ou, de façon mobile, sur un téléphone ou dispositif portable.

²⁵ Par exemple, IPVideoMarket.info recommande l'usage de grappes de stockage pour des réseaux comprenant au-delà de 48 caméras analogiques ou plus de six caméras mégapixel.
http://ipvideomarket.info/report/examining_the_future_of_video_surveillance_storage

Les grands centres d'opérations de sécurité, supervisant des centaines de caméras, utilisent souvent un mur d'écrans vidéo. Ceux-ci offrent une grande surface de visionnement et permettent d'afficher différents flux vidéo.

3.1.2 Évolution des systèmes de vidéosurveillance

La transition numérique en vidéosurveillance s'est opérée en plusieurs étapes. Amorcée avec l'apparition de l'enregistreur numérique, elle se poursuit vers une conversion totale à l'infrastructure IP, où la vidéo est transmise sur réseau intranet ou Internet de la caméra à l'écran de visionnement. Dans ce passage, l'on retrouve plusieurs systèmes hybrides, intégrant composantes analogiques et numériques. La figure ci-dessous présente les jalons importants qui ont marqué l'évolution vers la vidéosurveillance intelligente sur réseau IP.

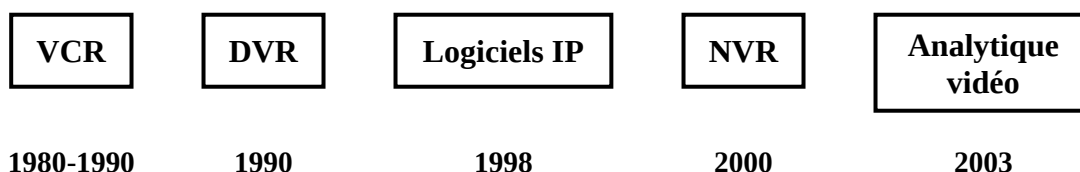


Figure 3 - Évolution du matériel de vidéosurveillance

3.1.2.1 Première génération : le tout analogique

Dans le réseau TVCF analogique traditionnel, des caméras analogiques sont connectées par câbles coaxiaux (un câble par caméra) aux écrans de surveillance et, pour des fins d'archivage, à un magnétoscope qui enregistre la vidéo sur cassette. Un multiplexeur peut être utilisé pour grouper les flux vidéo de plusieurs caméras en un seul signal composite qui est transmis au magnétoscope ou à un moniteur analogique. Il permet d'afficher quatre, neuf ou 16 signaux vidéo sur un même écran, ou d'enregistrer ceux-ci sur un même système d'archivage. Aucune compression n'est effectuée sur les signaux vidéo. Avec un magnétoscope conçu à cet effet, l'enregistrement à taux de trame (*frame rate*) réduit permet d'économiser de l'espace sur la bande vidéo, selon les besoins de surveillance²⁶.

- Avantages
 - Les systèmes analogiques sont très fiables
 - Simple à utiliser, ils ne requièrent pas de compétences informatiques.

²⁶ *Time lapse mode* permettant d'enregistrer à 15 fps (*frame per second*), 7.5 fps, 3.75 fps et 1.875 fps.

- Inconvénients
 - La qualité de la vidéo est inférieure à celle des systèmes numériques.
 - Il faut changer les cassettes fréquemment (aux trois jours ou plus).
 - Nécessite un nettoyage et un entretien régulier des magnétoscopes.
 - La qualité de la vidéo enregistrée se détériore avec le temps.
 - Ne permet pas le visionnement à distance, comme sur les réseaux numériques.
 - Ce sont des systèmes propriétaires.

3.1.2.2 Deuxième génération : le système hybride

Le remplacement du magnétoscope à cassette par un enregistreur numérique (DVR) représente la première étape de la transition numérique en vidéosurveillance. Apparus dans les années 90, les enregistreurs numériques archivent la vidéo sur des disques durs. Comportant souvent plusieurs entrées vidéo, l'enregistreur numérique remplace à la fois le multiplexeur et le magnétoscope analogique.

Les modèles récents sont équipés d'un port Ethernet, permettant la connexion à un réseau et l'accès à distance à la vidéo, soit en temps réel, soit à partir de l'enregistrement. Les transmissions vidéo se font sous protocole IP à partir de l'enregistreur numérique. Ils permettent la transition vers un système hybride de vidéosurveillance sur réseau IP, tout en conservant les caméras analogiques. L'enregistreur numérique hybride (HDVR), quant à lui, peut recevoir à la fois les flux vidéo de caméras analogiques et IP. Il représente une solution efficace pour moderniser un système de vidéosurveillance en profitant des avantages des nouvelles caméras IP, tout en conservant les caméras analogiques existantes en place. Alors qu'on estime que 95 % des caméras sont encore analogiques, les enregistreurs numériques et les enregistreurs numériques hybrides sont des technologies très répandues.

- Avantages
 - Aucune cassette à changer.
 - La vidéo archivée est de meilleure qualité, sans détérioration avec le temps.
 - Possibilité de chercher rapidement dans les enregistrements vidéo.
 - Surveillance vidéo et opération du système à distance à partir d'un PC.
- Inconvénients :
 - Concentration des tâches de numérisation, compression vidéo, enregistrement et réseautage dans la même machine.
 - L'enregistreur numérique est un appareil propriétaire, ce qui augmente les coûts de maintenance et de mise à jour.
 - Le nombre d'entrées vidéo de l'enregistreur numérique (souvent un multiple de 16) contraint l'ajout de caméras.

Les encodeurs vidéo, aussi appelés serveurs vidéo, sont utilisés pour convertir les signaux provenant de caméras analogiques et les transmettre en flux IP sur un réseau via un commutateur. Tout en conservant les caméras analogiques, ils permettent un passage presque complet à l'infrastructure réseau pour la vidéosurveillance, puisque que la vidéo est constamment transmise sous le protocole IP à travers le réseau.

Les encodeurs vidéo peuvent être utilisés avec les enregistreurs vidéo réseau (NVR). Ceux-ci ne peuvent traiter et enregistrer que des flux vidéo IP. Ils sont offerts sous une plateforme ouverte (un ordinateur muni d'un logiciel de gestion vidéo) ou dans un matériel propriétaire dédié. Sous cette dernière forme, l'enregistreur vidéo réseau se compare à un enregistreur numérique hybride, excepté qu'il nécessite l'usage d'encodeurs pour opérer avec des caméras analogiques.

- **Avantages**

- Utilisation d'ordinateurs et de matériel standards de réseau pour l'enregistrement et la gestion de la vidéo.
- Possibilité d'enregistrer à l'extérieur du site de surveillance (par exemple, centralisation des enregistrements).
- Architecture distribuée qui offre flexibilité, extensibilité (peut ajouter une caméra à la fois) et redondance (en cas de bris ou pannes).

- **Inconvénients**

- Gourmand en bande passante, si l'enregistrement est fait hors du site de surveillance (par ex., de façon centralisée).
- Si le réseau tombe en panne, l'enregistrement peut être interrompu.
- Si l'enregistrement centralisé n'est pas requis, l'utilisation d'enregistreurs vidéo réseau est souvent plus coûteuse que celle d'enregistreurs numériques.
- Nécessitent des calculs complexes pour déterminer le nombre de flux vidéo pouvant être supportés par le serveur, la quantité d'espace disque nécessaire à l'enregistrement, le taux de trames, le niveau de compression et d'autres facteurs liés aux capacités du réseau.

3.1.2.3 Troisième génération : le tout numérique IP

Au sens strict, un système de vidéosurveillance est complètement IP, lorsque toutes ses composantes sont numériques et toutes les transmissions sont effectuées sous le protocole IP. Ces réseaux comprennent donc des caméras réseau, aussi appelées IP. Il s'agit de caméras intégrant leur propre encodeur. Celles-ci sont reliées, via des commutateurs réseau, à des serveurs (ordinateurs personnels), munis d'un logiciel de gestion vidéo. L'enregistrement est fait sur serveur ou sur des enregistreurs vidéo réseau propriétaires. Les traitements sont effectués sur le serveur ou dans les périphériques. Toutefois, beaucoup de gens considèrent qu'un système de vidéosurveillance dont la vidéo est transmise sous

protocole IP à partir des encodeurs, constitue un système réseau IP. Dans ces systèmes, les caméras peuvent être analogiques, en autant qu'elles soient reliées à des encodeurs.

Plus de détails sur la vidéosurveillance IP et, notamment ses avantages et inconvénients, sont fournis dans la section suivante.

3.1.3 Vidéosurveillance IP

Depuis deux ans, le marché de la vidéosurveillance migre de la vidéo analogique à la vidéo IP. Cet essor de la vidéosurveillance réseau est favorisé par le perfectionnement des processeurs, la baisse des coûts de stockage et l'amélioration des algorithmes de compression.

Bien que cette transition s'observe, elle ne fait que débiter et il est difficile de prédire à quel rythme le « tout IP » prendra le dessus sur les technologies analogiques en vidéosurveillance. Les caméras constituent le facteur de résistance. En effet, il est estimé que 95 % des 40 millions de caméras installées à travers le monde sont encore analogiques [1]. De plus, encore aujourd'hui, seulement un acheteur sur quatre choisit des caméras IP²⁷. Pourtant, les caméras IP offrent des avantages techniques sur les caméras analogiques, tels qu'une meilleure qualité d'image, une résolution plus élevée et de l'intelligence embarquée. Le coût élevé des caméras IP, environ le double des caméras analogiques, reste le principal frein à l'achat. Avec les améliorations apportées par les manufacturiers aux enregistreurs vidéo et l'existence d'enregistreurs vidéo hybrides, le règne des caméras analogiques pourrait se prolonger encore quelques années.

Les réseaux IP de vidéosurveillance de dernière génération présentent les caractéristiques suivantes :

- Ils sont numériques de A à Z : caméras, réseaux, enregistrement, accès.
- Ils peuvent inclure différents types de caméras : intelligente, mégapixel, sans fil, PTZ, panoramiques, etc.
- Ils utilisent du matériel non propriétaire.
- Ils fonctionnent avec des serveurs distribués et multiplateformes.
- La sauvegarde se fait sur réseau (NVR).
- On peut y accéder à distance, n'importe où, n'importe quand, soit d'un centre de contrôle, via Internet ou un réseau LAN ou WAN, sur un cellulaire ou un assistant numérique personnel, etc.
- Ils peuvent inclure de l'analytique vidéo.

²⁷ IP Video Market Info, 2009.

La vidéosurveillance sur réseau IP offre de nombreux avantages. Elle repose sur une infrastructure plus souple que la vidéo analogique, combinant transmission câblée et sans fil. De plus, l'infrastructure réseau est rapide et facilement extensible. Il n'y a pas de limite au nombre de caméras qui peuvent s'y ajouter. Considérant que les systèmes actuels peuvent facilement comporter entre 400 et 500 caméras, comparativement à 25 à 30 il y a quatre ans, cette facilité d'étendre le réseau de vidéosurveillance est très attrayante lorsqu'on pense déployer un nouveau système.

Pour les installations étendues comportant de grandes distances entre les caméras et les systèmes d'enregistrement, les caméras IP deviennent un choix avantageux, car le coût du câble coaxial est très élevé. C'est pourquoi les caméras IP sont surtout déployées pour la surveillance d'institutions, telles que les établissements scolaires, les campus de grandes entreprises, les municipalités et les bases militaires.

Les caméras IP apportent de nombreux bénéfices techniques. Par exemple, les caméras mégapixel IP offrent des avantages indéniables au niveau de la vidéosurveillance. Ces caméras, présentant une résolution nettement supérieure à celle des caméras analogiques, ont le potentiel de résoudre plus de crimes. Bien que son coût soit élevé, une seule caméra mégapixel peut souvent remplacer plusieurs caméras. Les caméras intelligentes, intégrant des processeurs, apportent des gains techniques aux systèmes de vidéosurveillance de nouvelle génération. Elles permettent de distribuer les calculs pour les traitements d'analytique vidéo et, ainsi, de ménager la bande passante en ne transmettant que les données pertinentes pour la sécurité.

L'architecture ouverte des réseaux de vidéosurveillance IP permet de combiner le matériel de différents fabricants. Il est ainsi possible de sélectionner les composants les plus adaptées à son application de surveillance. De plus, l'architecture IP facilite l'intégration de différents systèmes de sécurité (vidéo, alarmes de feux, contrôle d'accès, etc.).

La configuration de ces réseaux avec redondance, tant au niveau de la transmission que de l'archivage, assure une meilleure fiabilité. Dans un réseau entièrement analogique, le mauvais fonctionnement d'une caméra ou d'un enregistreur peut signifier une perte définitive de vidéo. De plus, l'archivage sur réseau, dont les coûts ne cessent de baisser, permet de conserver des années de vidéo plutôt que quelques jours ou semaines avec les magnétoscopes ou enregistreurs numériques. Il suffit d'ajouter des disques durs pour augmenter la capacité de stockage.

Dans ces réseaux, la transmission numérique de la vidéo, de bout en bout du système, réduit les pertes de qualité qu'occasionnent les conversions d'analogique à numérique. De plus, par des traitements logiciels intelligents, il est possible de filtrer les événements pertinents dans la vidéo et de ne transmettre que les métadonnées les décrivant. Ceci permet d'économiser de la bande passante. Ces métadonnées servent ensuite à indexer le contenu vidéo pour permettre des recherches plus performantes dans les séquences captées. Il est aussi possible, dans ces réseaux, de transmettre des commandes aux caméras, en fonction

de la vidéo traitée. Par exemple, en réponse à un événement suspect, le logiciel de gestion vidéo pourra activer automatiquement le zoom optique ou numérique sur une caméra du réseau pour un suivi plus précis de la situation.

Le passage à la vidéosurveillance IP comporte tout de même certains inconvénients. Par exemple, dans le cas d'infrastructures analogiques existantes, refaire tout le filage réseau peut représenter un coût élevé. Dans ce cas, l'utilisation d'encodeurs pour numériser les signaux analogiques permet de conserver les caméras en place et d'implanter un réseau hybride. De plus, la technologie des enregistreurs numériques a beaucoup progressé, afin de rester compétitive. Les enregistreurs numériques offrent désormais plusieurs avantages comparables aux technologies sur réseaux IP : accès à distance, capacité de gérer un grand nombre de caméras, intégration avec les autres systèmes (contrôle d'accès, détection d'intrusion, systèmes de points de vente, etc.), capacité analytique. Pour de petites installations de vidéosurveillance, l'utilisation de caméras analogiques avec enregistreurs numériques offre donc un excellent rendement, à des coûts moindres que la vidéo IP.

Bien que sur le plan technologique, les réseaux IP de vidéosurveillance offrent de nombreux avantages, le déploiement de ceux-ci pose certains problèmes organisationnels. Le premier réside dans l'installation. La plupart des intégrateurs et installateurs en vidéosurveillance sont issus du secteur de la sécurité physique. Or, l'installation de systèmes de vidéosurveillance sur réseau IP requiert des compétences en technologie de l'information, particulièrement en réseautique. Encore peu d'intégrateurs et installateurs de vidéosurveillance sont spécialisés dans ce domaine.

Le second problème touche à la gestion de ces systèmes. Une fois installés, qui, dans l'organisation, est responsable du système de vidéosurveillance : le personnel de sécurité physique ou les services informatiques ? Le flou qui existe encore sur cette question dans les organisations retarde bien souvent le passage à la vidéosurveillance IP.

Finalement, passer d'un réseau de télévision en circuit fermé à un système de vidéosurveillance, dont les données transitent par les réseaux Ethernet ou Internet, soulève les questions de sécurité informatique. Évidemment, ceci nécessite de mettre en place les mécanismes de sécurité adéquats pour protéger la vidéo de surveillance. Aussi, le bon fonctionnement de la vidéosurveillance devient tributaire de la fiabilité du réseau. À cet égard, l'intégration de la vidéosurveillance sur réseaux IP suivra peut-être celle de la téléphonie IP, qui est maintenant bien répandue.

3.1.4 Architecture d'un réseau de vidéosurveillance intelligente

Les systèmes de vidéosurveillance intelligente peuvent être déployés selon deux grands types d'architecture, soit centralisée ou distribuée. L'une comme l'autre opèrent des traitements intelligents pour extraire des données sur les images vidéo et peuvent, au besoin, commander le déplacement d'une caméra PTZ pour opérer une surveillance active.

3.1.4.1 Architecture centralisée

Dans une architecture centralisée, tous les traitements intelligents sont concentrés en un même endroit. Dans les systèmes traditionnels, c'est l'enregistreur numérique qui récoltera tous les flux vidéo pour en faire l'analyse. Pour les infrastructures en réseau, c'est un serveur informatique (un PC) qui opérera les traitements analytiques.

L'analyse vidéo nécessite une grande puissance de calcul qui monopolise une part importante des ressources du processeur. Comme ils doivent aussi gérer l'encodage, l'enregistrement et le visionnement des flux vidéo, les enregistreurs numériques et serveurs ne peuvent accomplir des tâches d'analytique vidéo que sur un nombre restreint de caméras.

De plus, dans le cas des systèmes de vidéosurveillance sur réseau, la transmission de tous les flux vidéo en un point centralisé consomme beaucoup de bande passante. Le réseau informatique doit pouvoir soutenir ce trafic.

3.1.4.2 Architecture distribuée

Comme son nom l'indique, l'architecture distribuée répartit les traitements intelligents dans les différents nœuds du système de vidéosurveillance. Ainsi, les calculs nécessaires à l'analytique pourront être faits en périphérie, sur des caméras intelligentes dotées de processeurs, les encodeurs ou dans les commutateurs réseau. Dans cette architecture, plutôt que d'envoyer des flux vidéo à l'enregistreur numérique ou à un ordinateur central, seules des métadonnées extraites sur la vidéo sont transmises. L'intelligence peut aussi être partagée entre les périphériques et l'unité centrale de traitement.

Cette infrastructure aide à diminuer les coûts de câblage et la bande passante requise dans un réseau de vidéosurveillance. De plus, elle offre une meilleure extensibilité, puisque l'ajout de caméras n'est pas nécessairement limité par la puissance de calcul de l'enregistreur numérique ou du serveur.

3.2 État de l'avancement technologique en analytique vidéo

L'analytique vidéo et la vidéosurveillance intelligente sont des domaines de recherche très actifs. En particulier, depuis les dix dernières années, plusieurs conférences, éditions spéciales de revues ou articles y ont été consacrés. Quelques produits commerciaux ont vu le jour suite aux recherches menées dans ce secteur. De grands projets financés par les gouvernements, tels que VSAM, aux États-Unis et PRISMATICA, en Europe, ont favorisé le développement de techniques de détection, suivi et reconnaissance d'objet à partir de séquences vidéo.

Toutefois, il s'agit de technologies émergentes. Leur utilisation dans des applications à grande échelle reste encore récente et, somme toute, marginale. Le coût de ces

technologies, ainsi que leurs limites techniques actuelles pour la surveillance en environnements complexes, freine une adoption plus généralisée.

Cette section dresse un portrait de l'avancement technologique de la vidéosurveillance intelligente. Elle présente les principales analyses que les logiciels d'analytique vidéo peuvent accomplir. On y décrit sommairement les fonctionnalités actuellement implantées dans les systèmes commerciaux, ou en développement dans les laboratoires de recherche. Une énumération des principaux défis que confrontent ces technologies, ainsi que des besoins actuels et futurs qui sont envisagés par les utilisateurs, y est aussi présentée.

Une revue plus poussée des différents procédés et algorithmes d'analyse vidéo intelligente, ainsi qu'une bibliographie plus étendue du sujet, peuvent être trouvées dans les publications scientifiques [8, 9, 10, 11, 12, 14].

3.2.1 Description des techniques d'analytique vidéo

L'analytique vidéo consiste à reproduire, à l'aide d'un ordinateur, l'analyse qu'effectuerait un humain en regardant les séquences vidéo provenant de caméras de surveillance. Les logiciels d'analytique traitent les images d'un flux vidéo pour y détecter automatiquement les objets (personnes, matériel, véhicule) et les événements d'intérêt pour des fins de sécurité. Une fois détectés, les objets peuvent être identifiés, suivis et localisés (Figure 4). Leurs actions et interactions sont analysées et classées, afin d'interpréter l'activité d'une scène pour la soumettre à l'attention d'un opérateur humain.

Les logiciels d'analytique vidéo servent en deux modes, soit en temps réel et en temps différé. En temps réel, ils détectent, sur les flux vidéo, les situations représentant une menace à la sécurité et déclenchent une alarme. En temps différé, ils permettent de retrouver plus rapidement les séquences vidéo présentant un incident sous enquête.

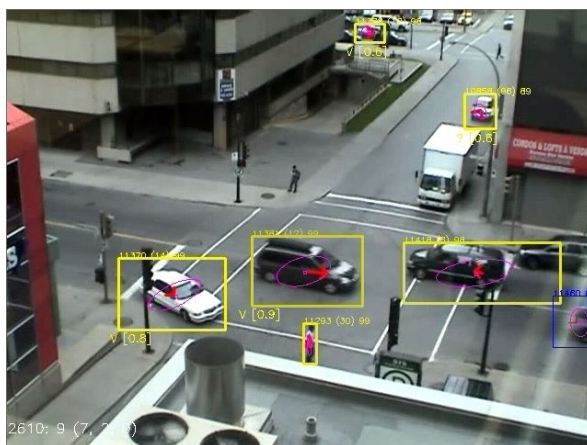


Figure 4 - Détection et suivi d'objets

Alertes en temps réel : La majorité des alertes sont définies par l'utilisateur du système de vidéosurveillance intelligente. Il peut s'agir d'alertes génériques, telles que la détection d'un objet abandonné ou d'un élément de la scène se déplaçant au-dessus d'un seuil de vitesse fixé. Pour déclencher ces alarmes, seules les propriétés de mouvements des objets sont analysées par le système. Des alertes plus spécifiques peuvent être lancées suite à la classification des objets ou de leur mouvement (par exemple, la discrimination entre le passage d'un humain ou d'un animal dans une zone extérieure). Les alertes comportementales basées sur la conformité ou non à un modèle de comportement enseigné au système (par exemple, un individu tentant d'ouvrir plus d'une voiture dans un stationnement), constituent des alertes prédéfinies.

Certaines alertes en temps réel sont identifiées automatiquement. Au fil du temps, le système apprend un modèle d'activité et finit par détecter les activités dérogeant de la norme. Par exemple, un logiciel d'analytique pourra apprendre que des véhicules circulent dans la rue et les piétons, sur le trottoir. L'inverse pourra sonner l'alarme.

Recherche de vidéo pour enquête : Les traitements d'analytique permettent d'indexer le contenu vidéo, en fonction de caractéristiques telles que la forme des objets, leur taille, leur apparence, leur trajectoire, leur type, ainsi que leur modèle d'activité. Stockées sous forme de métadonnées, ces informations permettront d'effectuer des recherches spatiotemporelles du type « trouver toutes les séquences où l'on voit une personne vêtue de rouge passer devant un certain édifice entre deux dates données ».

Les fonctions analytiques développées pour les systèmes de vidéosurveillance comportent différents niveaux d'analyse. Hiérarchiquement, elles s'exécutent du niveau des pixels, à celui des objets, pour atteindre l'échelle des comportements. Elles se regroupent selon les tâches suivantes :

1. Détection de changements
2. Segmentation d'objets en mouvement
3. Suivi d'objets
4. Classification et identification d'objets
5. Classification d'activités et de comportements

3.2.1.1 Détection de changements

En vidéosurveillance, la détection des changements dans une séquence vidéo est à la base de toute analyse intelligente. Elle pourra déceler une activité dans la scène sous surveillance, notamment le déplacement d'objets. De plus, elle peut révéler l'apparition ou la disparition d'un objet (objet abandonné ou volé). Elle s'utilise aussi pour signaler automatiquement les altérations accidentelles ou intentionnelles subies par une caméra : obstructions (poussière, toiles d'araignées, humidité, peinture, autocollants), réorientation, flou.

Beaucoup de techniques de détection de mouvements utilisées en analytique vidéo reposent sur la détection de changements. Or, détecter les changements dans une séquence vidéo ne cible pas spécifiquement le mouvement des objets, mais peut faire ressortir toute modulation de l'image. Pour segmenter²⁸ les objets se déplaçant, il faut parvenir à discriminer entre les fluctuations de la valeur des pixels correspondant à des mouvements cohérents et ceux provoqués par les changements environnementaux (Figure 5).



Figure 5 - Segmentation d'un individu dans une séquence vidéo

Il s'agit d'un problème majeur en analytique vidéo, car les environnements complexes peuvent présenter beaucoup de variations, parfois subites : changement d'illumination (ombres, mouvement du soleil, nuages, réflexions spéculaires dans les vitres ou sur l'eau, éblouissement provoqué par des sources lumineuses dans la scène), mouvements non pertinents (drapeau flottant au vent, vagues sur l'eau). C'est pourquoi beaucoup de méthodes analytiques fonctionnent bien à l'intérieur, dans des scènes présentant peu de mouvement. Beaucoup plus rares sont les algorithmes suffisamment robustes pour être appliqués en milieux non contrôlés.

Plusieurs techniques de segmentation de mouvements ont été proposées.

Soustraction de l'arrière-plan : Sous sa forme la plus primitive, la détection des changements se résume à trouver, pixel à pixel, les différences de couleur ou de texture entre les images d'une séquence. Une première catégorie de techniques consiste à comparer chaque trame d'une séquence à une image de référence, appelée arrière-plan, qui représente la scène sans perturbation. Les zones de changements sont formées des pixels présentant une différence d'intensité supérieure à un seuil. La soustraction pixel à pixel entre deux images est très sensible au moindre changement environnemental, comme les variations d'illumination et les mouvements inhérents à la scène (par exemple, le feuillage d'un arbre agité par le vent). Pour pallier ce problème, certaines techniques adaptent, en continu le modèle de l'arrière-plan aux fluctuations intrinsèques de l'environnement²⁹. La différence avec l'arrière-plan est une méthode qui convient surtout aux environnements internes, où

²⁸ La segmentation consiste à séparer les objets de l'arrière-plan.

²⁹ Par exemple, en utilisant un filtre de Kalman [9].

les conditions d'éclairage sont contrôlées et où il y a peu d'activité (par exemple, la surveillance d'un corridor).

Différence temporelle : Une seconde classe de méthodes de détection de changements se base sur une différenciation temporelle, entre quelques trames consécutives. Celles-ci s'adaptent aux variations dans le temps de l'environnement. En contrepartie, elles ont tendance à négliger certaines variations liées au mouvement d'objets dans la scène, surtout si ceux-ci se déplacent lentement. Elles produisent souvent des trous dans les objets détectés. Ces techniques nécessitent donc des traitements de lissage, avec des opérateurs morphologiques et le filtrage des trous et formes trop petites. Pour ne conserver que les mouvements significatifs et éliminer les mouvements occasionnels, certaines techniques dressent une carte des régions présentant un niveau élevé d'activité, en se basant sur le patron de mouvement.

Flux optique : Les méthodes analysant le flux optique³⁰ permettent de détecter les directions cohérentes de changements des pixels associées au mouvement d'objets dans la scène. Cependant, elles exigent des calculs complexes difficiles à exécuter en temps réel. De plus, le flux optique s'avère sensible au bruit³¹ de l'image.

3.2.1.2 Suivi d'objets

Après avoir détecté les objets en mouvement, les systèmes de vidéosurveillance intelligente suivent leur déplacement au cours d'une séquence vidéo (Figure 6). Cette tâche nécessite de localiser d'une image à l'autre chaque objet suivi. Il peut se faire en 2D, à partir d'une seule caméra, ou en 3D, en combinant deux vues dont la relation géométrique est connue.

Beaucoup de techniques de suivi se basent sur des méthodes mathématiques qui permettent de prédire la position d'un objet sur une trame à partir de son déplacement observé dans les trames précédentes³². Suivre plusieurs objets à la fois présente de nombreux défis. Chaque objet détecté dans une trame doit être associé à son correspondant dans la trame subséquente. Cet appariement s'effectue à partir des contours des objets, de leurs caractéristiques (par ex., coins, aire, ratios, etc.), ou de leur modèle d'apparence.

Les occlusions (régions cachées par d'autres), représentent une difficulté majeure pour le suivi d'objets. Un système de vidéosurveillance peut perdre la trace d'un objet, si celui-ci est totalement ou partiellement obstrué pendant une certaine période de temps. Il peut aussi être difficile de dissocier deux objets lorsqu'ils sont très proches ou que l'un cache l'autre.

³⁰ Le flux optique est le champ de vecteurs de déplacement produit dans l'image par des objets en mouvement dans une scène 3D.

³¹ Défauts de l'image souvent attribuables aux conditions d'acquisition et aux limites de la caméra.

³² Filtre de Kalman, filtres particuliers, réseaux bayesiens dynamiques, méthode géodésique, etc.

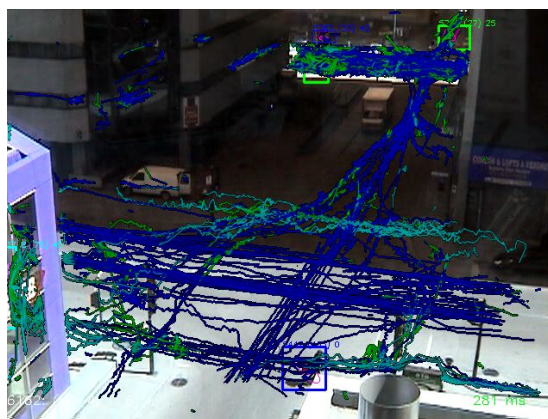


Figure 6 - Suivi de trajectoires d'objets sur une séquence vidéo

3.2.1.3 Classification et identification d'objets

Les objets détectés par un système de vidéosurveillance seront habituellement classés en différentes catégories : humain, véhicule, animal, etc. Ce classement peut s'effectuer préalablement au suivi pour ne conserver que les trajectoires des objets pertinents pour les fins de surveillance.

De façon générale, les systèmes reconnaissent la nature d'une entité détectée à partir de ses attributs de forme et de ses propriétés de mouvement. Par exemple, un humain se présente habituellement comme une forme plus haute que large, tandis qu'une automobile sera plus large que haute (Figure 7). La démarche humaine présente des caractéristiques particulières, notamment, une certaine périodicité.

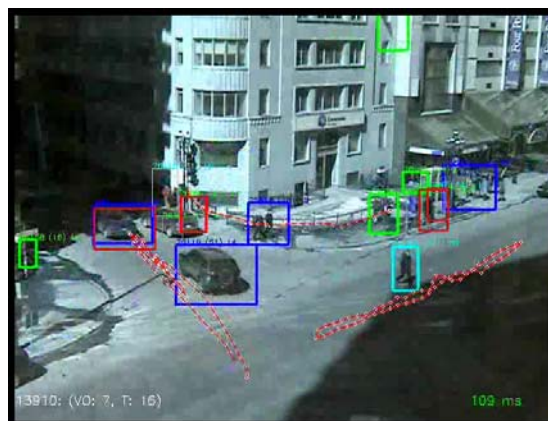


Figure 7 - Classification d'objets (humains vs véhicules)

L'identification d'objet pousse plus loin la reconnaissance. Après avoir trouvé la classe à laquelle appartient un objet, il s'agit de déterminer son identité. En surveillance, particulièrement pour le contrôle d'accès ou la recherche de suspect, on voudra, le plus souvent, reconnaître un individu ou décoder la plaque d'immatriculation d'une voiture. Beaucoup d'efforts de recherche et développement ont été investis, dans les dernières années, dans ces deux applications spécialisées.

La reconnaissance des visages et de la démarche humaine constituent les deux principaux outils biométriques utilisés pour l'identification de personnes en vidéosurveillance. L'analyse de la démarche fournit des indices pour une identification préliminaire d'un individu filmé de loin, en champ large.

La reconnaissance faciale permet une identification plus précise, mais nécessite une image du visage de bonne résolution et dans une pose adéquate (suffisamment de face). La plupart des systèmes toléreront une rotation du visage allant jusqu'à 45°. Depuis le début des années 90, plusieurs techniques pour l'encodage et la comparaison des visages ont été proposées³³. Elles reposent principalement sur l'extraction de descripteurs mathématiques ou de points topologiques du visage. D'abord développées à partir de photographies, les applications de reconnaissance faciale existent, depuis quelques années, sur des séquences vidéo. Selon la méthode utilisée, la reconnaissance peut être affectée par des changements d'apparence, tels que le port de lunettes ou de barbe, les expressions faciales et les variations d'illumination. Des nouvelles techniques de reconnaissance des visages en 3D³⁴, semblent améliorer la performance et la robustesse de l'identification, par rapport aux techniques 2D. Toutefois, la reconnaissance de visage en milieu non contrôlé, par exemple dans une foule, demeure un problème qui n'est pas encore résolu de façon satisfaisante par les systèmes actuels d'analytique vidéo.

La lecture de plaques d'immatriculation, à partir d'une vidéo de surveillance, est une application difficile. Elle nécessite une image de haute résolution. L'analyse d'image se confronte à de nombreuses interférences environnementales : intempéries, brillance des phares, saletés et dommages sur la plaque. Pour lire une plaque d'immatriculation, un système doit d'abord localiser le rectangle de la plaque parmi tous les détails de l'image (Figure 8). Il doit ensuite procéder à une reconnaissance automatique des caractères³⁵. Une plaque filmée à angle entraîne une distorsion des caractères dans l'image qui complique le processus de reconnaissance. Afin d'en maximiser l'efficacité, la reconnaissance de plaques se fait le plus souvent au moyen de systèmes spécialisés soignant le positionnement des caméras et la qualité de l'éclairage.

³³ Un survol des techniques de reconnaissance de visage est disponible sur <http://www.face-rec.org/algorithms/>

³⁴ Utilisation de lumière structurée infrarouge par A4Vision, ou de triangulation à partir de vues multiples par Geometrix.

³⁵ OCR, en anglais.



Figure 8 - Détection d'une plaque d'immatriculation

3.2.1.4 Classification d'activités et de comportements

Un des objectifs de la vidéosurveillance est d'interpréter les comportements individuels des objets d'une scène, ainsi que leurs interactions. Au sens large, les comportements se définissent comme les actions observables d'agents (humains, animaux, véhicules, etc.). Comme la tâche de reconnaissance de comportements requiert une analyse sémantique, parfois complexe, de ce qui apparaît dans l'image, elle représente le défi le plus coriace pour les systèmes d'analytique vidéo.

On peut vouloir détecter un comportement simple, tel que « un individu a laissé un sac dans une salle ». Néanmoins, la chaîne d'interactions peut se complexifier rapidement :

Un individu A laisse un sac dans une salle. Un individu B prend le sac et sort de la salle. L'individu B croise l'individu A et lui sert la main. Conclusion, le sac n'a pas été volé.

L'analyse et l'interprétation de comportements nécessitent de reconnaître des patrons de mouvements et d'en dégager, à un plus haut niveau, une description des actions et interactions. Comme dans tout problème de classification, il s'agit d'associer une séquence de caractéristiques observées, à une séquence modèle représentant un comportement spécifique. Le problème consiste donc à modéliser les comportements typiques, par apprentissage ou par définition, et à trouver une méthode de comparaison tolérant des variations légères.

Parmi les techniques les plus utilisées pour modéliser les comportements normaux et détecter les comportements déviants, on note les modèles markoviens cachés³⁶, les réseaux de neurones et les réseaux bayesiens. Ces techniques génèrent une alarme sur la base de la

³⁶ En anglais, Hidden Markov Models (HMM).

divergence statistique au modèle inféré de la scène. Des méthodes de détection d'événements prédéfinis existent aussi. Elles se basent sur un système de règles. Par exemple, générer une alarme si un objet de taille supérieure à un seuil reste stationnaire pour plus d'un certain temps dans une région donnée.

3.2.1.5 Analyse de foule

Un domaine d'avenir pour la recherche en analytique vidéo repose sur l'analyse et la surveillance de foules. Avec l'accroissement rapide de la population mondiale, la densification des grands centres urbains et le problème grandissant d'assurer la sécurité lors de grands rassemblements, la vidéosurveillance offre une avenue intéressante. Les caméras sont d'ailleurs déjà utilisées pour surveiller les grands événements (par exemple, événements sportifs³⁷, congrès politiques, etc.), mais l'efficacité analytique des systèmes vidéo, dans ce contexte, reste encore discutable.

Zhan et al. [14] présentent une revue de la recherche en analyse de foule. Les différentes étapes d'analytique vidéo exposées dans les sections précédentes y sont appliquées. Toutefois, l'analyse d'une foule présente des problèmes particuliers, parce que celle-ci est composée de nombreux individus.

L'estimation de la densité représente une étape fondamentale pour la surveillance et la gestion de foule. Elle requiert d'évaluer, au moins approximativement, le nombre d'individus. Les nombreuses occlusions et juxtapositions rendent difficile la segmentation de piétons pour le dénombrement. Certaines techniques assument une relation proportionnelle entre le nombre de pixels associés à l'avant-plan, suite à la segmentation, et le nombre de personnes. D'autres méthodes se basent sur la texture de l'image pour caractériser la densité de la foule. Certains algorithmes détectent le contour des têtes. D'autres utilisent des histogrammes de plusieurs caractéristiques pour déduire le nombre approximatif de personnes.

Bien que le suivi d'objet soit l'un des sujets de recherche les plus populaires en vidéosurveillance, la plupart des algorithmes développés s'appliquent à un petit nombre de personnes (moins de dix à la fois). Le suivi de piétons dans des foules présente des difficultés majeures, notamment en regard du nombre élevé d'individus à suivre d'une trame à l'autre et des nombreuses occlusions présentes. Certaines méthodes font le suivi de points saillants, moins sujets à être perturbés par les occlusions que les contours. D'autres modélisent le corps humain ou ses parties. Des méthodes probabilistes d'appariement ou des filtres particuliers sont utilisées pour suivre ces modèles au cours d'une séquence vidéo. Il existe quelques travaux sur le suivi à partir de plusieurs caméras : M2Tracker

³⁷ Déjà en 2001, la ville de Tempa (Floride), avait utilisé la vidéosurveillance pour la reconnaissance faciale des membres de l'assistance. Tiré de Barber, G, *Living on the Wrong Side of a One-Way Mirror: Face Recognition Technology and Video Surveillance*, 16 juillet 2001. <http://www.graysonbarber.com/pdf/WrongSide.pdf>.

travaille avec des caméras synchronisées, et Chang et al.³⁸ utilisent une combinaison de caméras fixes et PTZ.

À des fins de sécurité, il est important de surveiller les mouvements d'une foule. On analysera, par exemple, sa trajectoire et son flux. Pour la modélisation de la foule et de ses comportements, certains chercheurs considèrent la foule comme un tout dont ils interprètent les mouvements des différentes portions. Des techniques, telles que le flux optique et les modèles markoviens cachés, sont utilisées pour modéliser les mouvements. Certains modèles vont combiner l'analyse microscopique (les individus) et macroscopique (la foule). Dans ce contexte, deux types d'approches sont proposées pour décrire l'activité d'une foule : l'application de modèles physiques, tels que la cinématique des particules dans un gaz et la dynamique des fluides, et des techniques basées sur les agents.

3.2.1.6 Vidéosurveillance active dans les systèmes multi-caméras

Les systèmes modernes de vidéosurveillance, particulièrement sur réseaux IP, peuvent comprendre des centaines de caméras. Parfois, plusieurs caméras couvrent une même zone. Certaines d'entre elles sont motorisées et peuvent être contrôlées pour capter plus de détails sur un événement détecté en champ large. Par exemple, la caméra pourra zoomer sur un individu pénétrant dans une zone, afin de permettre de l'identifier. Dans certains réseaux, les caméras sont intelligentes, c'est-à-dire qu'elles possèdent leur propre unité de traitement. Elles peuvent échanger de l'information avec un système central ou directement entre elles.

Ces réseaux de caméras de surveillance permettent de suivre des objets sur des zones étendues. De plus, les vues multiples peuvent servir à résoudre les problèmes d'occlusion d'objets. Dans une architecture distribuée, les traitements analytiques peuvent se faire en parallèle, accélérant l'analyse et économisant la bande passante en ne transmettant que des métadonnées.

Toutefois, ces réseaux soulèvent aussi des problèmes particuliers que le monde scientifique tente de résoudre :

- **Calibrage des caméras** : Opération qui consiste à établir la correspondance entre le repère global de la scène observée et le repère de la caméra, ainsi que de déterminer les paramètres intrinsèques de la caméra, comme la distorsion³⁹. Ce processus de précision peut s'avérer fastidieux pour un réseau comprenant de nombreuses caméras. Il est souhaitable de développer des fonctions analytiques ne requérant aucun calibrage ou des méthodes d'auto-calibrage des caméras.

³⁸ Cité dans [14].

³⁹ Tiré de http://wcours.gel.ulaval.ca/2008/a/19263/default/5notes/modele_camera.pdf.

- **Détection de mouvement** : Pour une caméra motorisée, le mouvement de la caméra crée un changement apparent dans l'image. Les méthodes de détection de mouvement doivent discriminer les changements indépendants du mouvement de la caméra.
- **Suivi d'objet sur plusieurs caméras** : Pour pouvoir suivre un objet d'une caméra à l'autre, il est nécessaire d'établir la correspondance entre les différentes vues dans un référentiel commun. Le recalage de caméras consiste à calculer les paramètres qui permettent de transformer l'image d'une caméra à l'autre, en fonction du changement de référentiel et du modèle de mouvement. Cette opération utilise une connaissance a priori de la topologie de la scène. Elle permet d'obtenir une vue 2D augmentée (2D1/2) ou 3D de la scène. La variation de l'apparence et de la pose des objets dans le temps, tout comme les changements d'illumination, compliquent le recalage.
- **Détection des altérations subies par les caméras** : Plus les réseaux comportent de caméras, plus il devient ardu de contrôler leur état de fonctionnement. Ces systèmes doivent intégrer des outils de détection automatique des bris et altérations des caméras, afin de demeurer fonctionnels.

Les systèmes de vidéosurveillance active multi-caméras sont surtout utilisés pour la surveillance d'aires étendues ou distribuées, telles que les systèmes de transport, les infrastructures bancaires, les établissements gouvernementaux (bases militaires, prisons, infrastructures stratégiques, centre de radars, hôpitaux), les édifices publics, les centres commerciaux et les stationnements.

3.2.2 Analytique dans les systèmes commerciaux

Depuis le début des années 2000, plusieurs produits d'analytique vidéo ont été mis sur le marché, afin de permettre une vidéosurveillance intelligente. Une liste des principaux développeurs de logiciels d'analytique vidéo est fournie à l'Annexe 4.

Dans l'ensemble, les produits disponibles offrent sensiblement les mêmes fonctionnalités de base. Certains logiciels se distingueront par quelques fonctionnalités plus spécialisées (par ex., reconnaissance de plaques d'immatriculation) ou par leurs performances.

Globalement, les principales fonctions d'analytique vidéo disponibles sur le marché se résument à :

- Suivi par caméra PTZ activé sur alarme.
- Détection de bris et d'altérations subis par les caméras.
- Détection d'objet disparu ou abandonné
- Détection d'intrusion (personne ou véhicule) dans des aires ou périmètres contrôlés : limites virtuelles interdites, zones de sécurité, passage de plusieurs individus ou véhicules à un contrôle d'accès sous une seule identification (*tailgating*), intrusion par une voie de sortie, personne passant par dessus ou dessous une guérite.

- Détection et suivi de personnes ou véhicules : analyse de la vitesse et direction de déplacement, détection de personne/voiture/objet stationnaire près d'une infrastructure sensible.
- Comptage de personnes ou véhicules, détection d'attroupements ou surnombre.
- Détection de vols et de fraudes aux points de ventes.
- Reconnaissance de comportements : détection de rôdeurs, bagarre, course, chutes, déplacement à contresens, graffitis, vandalisme.
- Monitoring de trafic : vitesse/densité/direction du trafic, accidents, objets sur la chaussée, limites de vitesse enfreintes, congestion, piétons, etc.
- Détection et reconnaissance de visages.
- Reconnaissance de plaques d'immatriculation.
- Détection d'incendies par analyse d'images.

Les technologies d'analytique vidéo sont encore jeunes et appelées à se développer. Beaucoup d'applications commerciales fonctionnent bien dans des environnements contrôlés. Toutefois, la plupart d'entre elles performant moins bien lorsque déployées chez les clients, dans des cas réels d'utilisation. De nombreux ajustements et paramétrages sont souvent nécessaires pour amener ces systèmes à opérer correctement pour une application spécifique.

Des fonctions de base, telles que la détection de mouvement, l'amélioration d'image et la détection d'altérations sur les caméras, sont en général assez robustes pour fonctionner dans une gamme étendue d'applications. Le comptage de personnes, la détection d'intrusion (limites virtuelles) et la reconnaissance de plaques d'immatriculation constituent des analyses suffisamment matures. Bien qu'elles nécessitent certains paramétrages, leur usage se répand.

De façon générale, les techniques de détection et de suivi d'objet se sont grandement développées en recherche et certaines d'entre elles sont intégrées dans des systèmes commerciaux, pour des cas simples d'utilisation. Toutefois, beaucoup de travail reste à faire pour développer ces techniques à des niveaux de performance et de robustesse nécessaires pour l'opération en environnements complexes. La détection et le suivi d'objet dans des foules, ou à travers un réseau de multiples caméras, constituent des problèmes difficiles.

Il existe plusieurs produits commerciaux spécialisés pour la détection et reconnaissance d'images (voir Annexe 4). Leur efficacité dépend largement de l'application et de la complexité des environnements dans lesquels ils doivent opérer. Généralement, ces technologies requièrent de contrôler les conditions d'acquisition (éclairage, pose, etc.) pour fournir des résultats satisfaisants.

Certains comportements sont détectés par les logiciels d'analytique sur le marché. Il s'agit d'activités pouvant être déduites de propriétés de mouvements simples (vitesse, direction, etc.), telles que, personne courant, rôdant ou tombant. Toutefois, il est souvent difficile de discriminer le niveau de menace que représente ce mouvement. Par exemple, une personne coure-t-elle parce qu'elle s'enfuit ou parce qu'elle ne veut pas rater son vol à l'aéroport? La reconnaissance de comportement demeure un domaine expérimental en analytique.

Les attentes face à l'analytique vidéo dépassent souvent largement l'efficacité des technologies actuelles. De plus, celles-ci s'avèrent complexes à intégrer et à utiliser. À ce sujet, Hearing et al. [11] suggèrent une liste de caractéristiques souhaitables pour un système commercial d'analytique vidéo.

- **Minimiser les configurations nécessaires** : Un système commercial ne devrait pas nécessiter beaucoup de temps en configuration, paramétrage et entraînement. Idéalement, l'utilisateur devrait fournir un minimum d'informations supplémentaire au flux vidéo lors de l'installation.
- **Offrir une performance adéquate** : Le nombre de fausses alarmes doit être maintenu aussi bas que possible pour éviter de déranger le personnel de sécurité inutilement. Par contre, il est encore plus critique que le système ne laisse pas passer une menace réelle. L'équilibre à viser entre le nombre de fausses alarmes et celui des détections manquées dépend de l'application de sécurité.
- **Ne pas nécessiter de calibrage des caméras ou automatiser celui-ci** : Le calibrage des caméras permet de calculer la taille et la vitesse réelles des objets de la scène. Il établit la correspondance entre la géométrie de la scène et celle de l'image.
- **Supporter une vaste gamme de caméras** : L'analyse vidéo devrait pouvoir se faire indifféremment sur les images provenant de caméras couleur, noir et blanc, infrarouge, thermique ou omnidirectionnelle.
- **Demeurer aussi générique que possible** : Idéalement, la détection d'événements pertinents devrait fonctionner dans des environnements variés et dans différents cas d'application. Toutefois, certains milieux recèlent des problèmes très spécifiques, tels que les zones comprenant des plans d'eau. Le mouvement de l'eau et les réflexions spéculaires perturbent les algorithmes de détection de changements dans l'image sur lesquels se base la détection et le suivi d'objets.
- **Offrir des mécanismes de protection de la vie privée** : Les systèmes d'analytique devraient permettre de masquer les détails sur les séquences vidéo (les visages, par exemple) qui ne sont pas essentiels au traitement d'une alarme de sécurité.

3.2.3 Besoins et défis en analytique vidéo

Suite à la recherche documentaire et la consultation d'experts et d'utilisateurs, quelques besoins et défis technologiques ont été identifiés pour le domaine de la vidéosurveillance intelligente. Ils sont présentés dans cette section.

Considérant l'explosion de la quantité de vidéo captés pour la sécurité, tous notent la nécessité de développer des méthodes automatisées de détection de personnes, d'objets ou d'événements suspects, afin de ne soumettre que les séquences pertinentes à l'analyse humaine. Les techniques existantes sont prometteuses, mais peu d'entre elles sont actuellement déployées commercialement dans des cas réels d'utilisation.

Au niveau de la recherche, il existe beaucoup d'algorithmes applicables à la vidéosurveillance, mais il s'agit souvent de solutions partielles n'attaquant qu'un segment du problème de la vidéosurveillance. Il existe peu de systèmes expérimentaux complets, opérant dans des conditions proches de la réalité.

Pour le moment, tous conviennent que ce qui fonctionne bien en analytique vidéo est la détection de mouvement, la détection d'objets spécifiques, la reconnaissance de plaques d'immatriculation effectuée à partir de systèmes spécialisés et la détection de certains comportements spécifiques (marche, course, porter un objet).

Voici ce qu'il reste à développer ou améliorer :

- La détection et la reconnaissance presque en temps réel, c'est-à-dire dans les quelques minutes suivant l'incident (surtout important pour la sécurité des infrastructures sensibles ou lors de grands événements).
- Plus spécifiquement, la reconnaissance de visages en temps réel (25 à 30 trames/sec).
- La reconnaissance de visages dans une foule. Ceci nécessite une image de résolution suffisante qui devrait être accessible avec les caméras mégapixel maintenant disponibles sur le marché.
- Le comptage de personnes dans des environnements peuplés et sous divers angles de vues.
- Le suivi d'objets spécifiques dans des scènes chargées (individu dans une foule ou véhicule dans le trafic).
- Le suivi de corps articulés pour la compréhension d'activités.
- La reconnaissance de comportements plus complexes, pertinents pour les fins de sécurité.
- La segmentation des régions de couleurs. Par exemple, l'information de couleur sur une voiture peut améliorer la performance de l'algorithme de reconnaissance de plaque. Elle peut aussi servir à reconnaître les différents morceaux de vêtements d'un individu.
- Pour la détection et la reconnaissance, miser sur la fusion de différentes données vidéo (par exemple, combiner reconnaissance faciale avec reconnaissance de la démarche), ou la fusion des données vidéo avec celles obtenues par différents systèmes (capteurs de température, systèmes biométriques, etc.).

Beaucoup d'algorithmes d'analytique vidéo fonctionnent seulement pour des caméras fixes, de bonne résolution et avec un éclairage adéquat et constant, ce qui s'avère très peu utile pour la majorité des applications. Certains problèmes fréquents ne sont jamais pris en considération, tels que les altérations subies par les caméras (toiles d'araignées, poussière,

caméra déplacée). Il s'avère primordial d'améliorer la robustesse et la précision de la plupart des algorithmes de détection, de suivi et de reconnaissance existants, en présence de conditions changeantes de l'environnement. Pour être adoptés par les consommateurs, les systèmes de vidéosurveillance intelligente devront être robustes aux différentes conditions météorologiques, s'ajuster aux changements d'illumination (naturelle et artificielle) de la scène et s'adapter aux pannes matérielles et logicielles.

Ceci pose un défi de taille pour le développement des systèmes de vidéosurveillance intelligente, soit celui de l'évaluation des performances. Les systèmes doivent-ils être comparés aux humains? Pour beaucoup de tâches de surveillances, telle que la détection d'objets abandonnés, les humains performant piètrement. Or, il est difficile de comparer les systèmes entre eux, car la plupart des tests de performance sont effectués sur des jeux de données différents.

Il serait donc souhaitable de développer des méthodes objectives et systématiques pour évaluer et comparer la performance des systèmes de vidéosurveillance intelligente. Cette opération dépend beaucoup de la tâche analytique à évaluer. De plus, ceci requiert de construire un jeu de données annotées (vérité terrain) et de choisir une mesure de distance pour évaluer l'écart entre les réponses du système et la vérité terrain.

Voici quelques initiatives d'évaluation de systèmes d'analytique vidéo déjà existantes :

- PETS (Performance Evaluation of Tracking and Surveillance)⁴⁰ : Permet de soumettre un algorithme en ligne pour évaluation. Propose une métrique.
- CREDS (Challenge for real time event detection solutions) : Concours pour la détection des événements prédéfinis sur des séquences de surveillance du métro de Paris (par ex., personne marchant sur les rails).
- I-LIDS (Imagery Library for intelligent Detection Systems)⁴¹ : Lancé par le Home Office Scientific Development Branch de Grande-Bretagne. Permet de tester sur des données vidéo pour la détection de véhicules stationnés, de bagages abandonnés, d'intrus dans des périmètres contrôlés et la surveillance de portes.
- ETISEO (Évaluation du traitement de l'interprétation de séquences vidéo)⁴² : Par le gouvernement français, projet terminé, mais corpus disponible sur demande pour des fins de recherche non commerciales.
- FRVT (Face Recognition Vendor Tests)⁴³ : Procède à des tests de différents systèmes de reconnaissance faciale sur plusieurs bases de données, afin d'offrir une comparaison objective entre les vendeurs. Les résultats permettent au gouvernement américain et aux

⁴⁰ www.petsmetrics.net.

⁴¹ <http://scienceandresearch.homeoffice.gov.uk/hosdb/cctv-imaging-technology/video-based-detection-systems/i-lids/i-lids-datasets-pricing/>.

⁴² <http://www.sop.inria.fr/orion/ETISEO/>.

⁴³ <http://www.frvt.org>.

agences de sécurité de savoir où les technologies de reconnaissance faciale peuvent être déployées et d'identifier les axes futurs de recherche dans ce domaine.

Finalement, les algorithmes d'analytique devront s'adapter aux nouvelles architectures des systèmes de vidéosurveillance : multi-caméras hétérogènes (potentiellement motorisées), intelligence distribuée, vidéo à haute résolution. De la recherche et du développement seront nécessaires pour :

- Introduire l'intelligence dans les caméras.
- Créer des algorithmes adaptatifs.
- Permettre le suivi par des caméras motorisées dans une approche multi-échelle : détection en champ large, puis zoom sur un objet ou un individu pour extraire plus de détails.
- Développer des algorithmes d'auto-adaptation et d'auto-calibrage pour ajuster en temps réel les paramètres des caméras (zoom, focus, ouverture, etc.), en fonction des changements de la scène surveillée.

3.3 Tendances technologiques pour la vidéosurveillance

Encore beaucoup des systèmes actuels de vidéosurveillance reposent sur des technologies traditionnelles : caméras analogiques, câbles coaxiaux, enregistreurs numériques. Toutefois, les progrès techniques dans ce domaine entraînent des changements dans les architectures, les composantes et les capacités des systèmes de vidéosurveillance.

Voici les principales tendances technologiques envisagées par les experts du domaine pour les prochaines années.

- Un passage à la vidéosurveillance sur réseaux IP s'opère. Surtout adoptée, présentement, pour les grandes infrastructures, la vidéosurveillance IP pourrait gagner la faveur de plus petits utilisateurs si les coûts des caméras IP baissent.
- Les caméras mégapixel constituent une avancée technique majeure pour la vidéosurveillance, offrant une meilleure résolution et une couverture plus large. De plus, elles améliorent le rendement des traitements analytiques. Elles devraient donc se répandre. Un expert questionné pour ce rapport prédisait que, d'ici 2012, la moitié des caméras de surveillance seront de haute résolution.
- Le standard de compression H.264 (MPEG-4 Part 10/AVC for Advanced Video Coding) devrait s'imposer en vidéosurveillance. Les taux de compression supérieurs qu'il offre par rapport aux standards existants permettent d'économiser bande passante et espace de stockage. Ce standard devrait favoriser l'adoption des caméras mégapixel en vidéosurveillance.

- Les systèmes de surveillance comprendront des réseaux de multiples caméras opérant en temps réel. Dans ces systèmes, la tendance est à distribuer les enregistrements et les traitements dans les différents nœuds (caméras et encodeurs), afin de diminuer la quantité de données transmises.
- Il devrait y avoir une plus grande intégration et une meilleure interopérabilité des différents systèmes de sécurité pour permettre leur gestion sous un même centre de commande et contrôle. Ainsi, la vidéosurveillance, le contrôle d'accès, les solutions biométriques, RFID, les systèmes de détection d'intrusion pourraient être reliés.
- La vidéosurveillance intelligente devrait progresser et les produits d'analytique vidéo devenir plus robustes et efficaces pour les applications de sécurité. La détection, le suivi et la reconnaissance d'objets (personnes, visages, véhicules, etc.) dans des scènes chargées, ainsi que la reconnaissance de comportements, seront les domaines de recherche les plus actifs pour la vidéosurveillance.
- L'utilisation des systèmes de vidéosurveillance dépassera de plus en plus le cadre de la sécurité. Des applications se développeront pour les analyses marketing, l'étude des comportements des consommateurs et la surveillance des opérations d'entreprises.

4. PORTRAIT DU MARCHÉ DE LA SÉCURITÉ ET DE LA VIDÉOSURVEILLANCE

4.1 Marché global de la sécurité

Le marché de la sécurité est un marché vaste et éclectique qui recouvre plusieurs activités au niveau de l'industrie (fabrication, services, intégration, distribution, etc.). L'offre peut également être divisée en divers segments de marché : sécurité des personnes, sécurité informatique, des réseaux et des communications (sécurité des TI), sécurité des infrastructures, contrôle d'accès, authentification, services de première ligne incluant les secours d'urgence et les interventions lors de crises, lutte contre le terrorisme, sécurité des transports (aériens, maritimes, ferroviaires, routiers), sécurité industrielle, détection et réponse à une attaque chimique, biologique, radiologique et nucléaire, etc. Il est à noter que de nombreux segments identifiés ont l'État pour moteur principal, ce qui illustre l'importance de cet acteur dans l'orientation du marché, tant à titre de législateur qu'à celui de client.

Plusieurs des produits ou des services offerts au sein des segments mentionnés ci-dessus se chevauchent, ce qui souligne les difficultés en lien avec la définition de ce marché et de ce qu'il comprend. Actuellement au Canada, aucune nomenclature officielle ne semble avoir été adoptée pour désigner le domaine de la sécurité

On peut noter à cet égard, l'approche du Centre des sciences pour la sécurité (CSS), une organisation publique fédérale gérée conjointement par Recherche et développement pour la défense du Canada et Sécurité publique Canada, et à laquelle collaborent 19 organismes

gouvernementaux fédéraux. Ayant essentiellement une mission de protection civile et publique, le CSS divise ses activités de S&T en quatre grands ensembles, soit :

- protection des infrastructures essentielles (PIE) ;
- surveillance, renseignement et interdiction (SRI) ;
- gestion des urgences et intégration des systèmes (GUIS) ;
- protection contre les agents chimiques, biologiques, radiologiques, nucléaires et explosifs (CBRNE).

Dans ce contexte, l'analyse de la taille de ce marché, ainsi que des revenus qu'il génère sur la base des différentes études publiées, s'avère complexe. La définition donnée au marché, c'est-à-dire ce qui y est inclus et ce qui ne l'est pas, varie d'une étude à l'autre, rendant la comparaison difficile. Malgré ce fait, le présent rapport présente les principales données disponibles, afin de fournir une idée de l'importance du marché de la sécurité et de ses tendances de croissance.

Selon un rapport de Homeland Security Research Corporation, le marché de la sécurité publique et civile a connu une phase de croissance très significative, de l'ordre de 600 % entre 2000 et 2008⁴⁴, notamment dans la foulée des attentats de septembre 2001. Il est important de noter que, dans cette étude, une définition très large de ce qui constitue le marché de la sécurité est utilisée en y incluant, par exemple, certaines dépenses en lien avec les activités de protection du territoire menées par les ministères de défense. Une croissance de 81 % de ce marché entre 2008 et 2018 est envisagée. Cette étude couvre 20 marchés nationaux clés qui définissent la tendance dans ce domaine.

Le Canada, même s'il ne constitue pas un joueur majeur à l'échelle internationale en matière de sécurité, a suivi la tendance à la hausse des dépenses en sécurité publique suite aux événements de New York et également en réponse aux réorganisations administratives du gouvernement fédéral des États-Unis et la création du Department of Homeland Security. Depuis sa création en 2003, le ministère de la Sécurité publique et de la Protection civile (SPPCC à l'époque et maintenant Sécurité publique Canada) s'est vu allouer annuellement des budgets entre cinq et sept milliards de dollars (Figure 9). Une étude plus approfondie des dépenses effectuées par ce ministère et les organisations qui le composent⁴⁵ serait toutefois nécessaire pour déterminer plus précisément leur destination.

⁴⁴ Homeland Security Research Corporation. National Security Spending Outlook in 20 countries, 2009-2018, 13 novembre 2008, disponible à : <http://www.homelandsecurityresearch.net/2008/11/13/national-security-spending-outlook-in-20-countries-2009-2018/>.

⁴⁵ Gendarmerie royale du Canada, Service correctionnel du Canada, Agence des services frontaliers du Canada, Service canadien du renseignement de sécurité, Commission nationale des libérations conditionnelles, Commission des plaintes du public contre la GRC, Bureau de l'enquêteur correctionnel, Comité externe d'examen de la GRC.

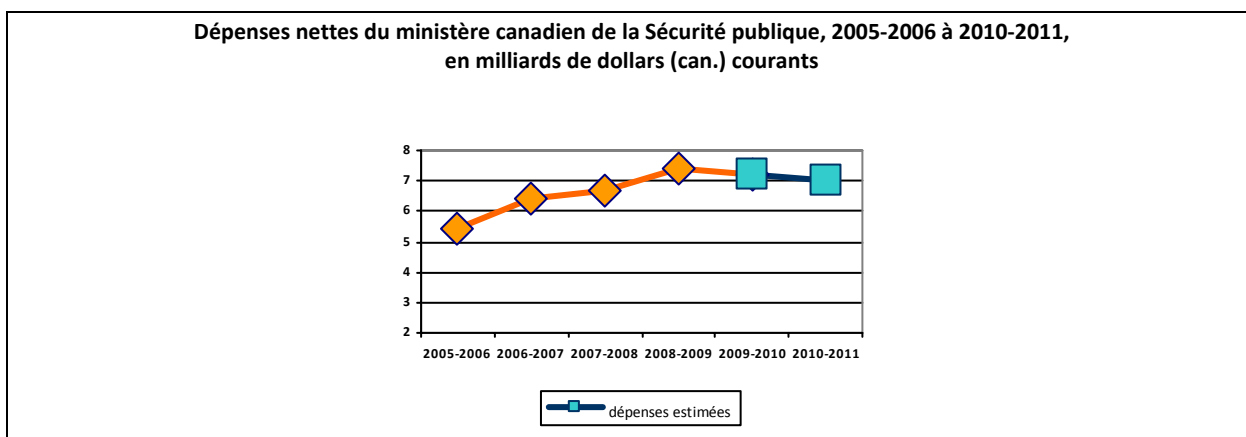


Figure 9 - Tableau tiré du rapport sur les plans et priorités, 2005-2006 à 2008-2009

Les données disponibles tendent ainsi à indiquer que la croissance des marchés continuera d'être au rendez-vous à l'échelle mondiale, mais que celle-ci sera peut-être plus mesurée qu'au cours des huit dernières années.

Plusieurs facteurs peuvent expliquer ce phénomène. Parmi les plus importants, mentionnons que la croissance observée dans la première moitié de la décennie 2000 a été pour beaucoup tributaire des vastes investissements publics dégagés par le gouvernement américain dans le cadre de la mise en œuvre du Homeland Security et des divers programmes de sécurisation du territoire. Une partie de ces derniers comprenait d'importantes immobilisations. Par exemple, mentionnons le programme Secure Border Initiative (SBI-net) ayant pour objectif la sécurisation des frontières nord et sud des États-Unis. La portion du programme dédiée à la frontière canado-américaine en est actuellement au stade du déploiement, les contrats pour la maîtrise d'œuvre du programme ayant été octroyés en 2006 à l'entreprise Boeing.

4.2 Marché de la vidéosurveillance

Le marché de la vidéosurveillance s'inscrit dans le marché de la sécurité et chevauche plusieurs des segments présentés dans la section précédente. Par exemple, aux États-Unis, en 2007, le segment de la vidéosurveillance représentait 34 % du marché national de la sécurité, évalué à 9,5 milliards de dollars⁴⁶.

⁴⁶ United States Security Market Report and Economic Impact Study, SIA, <https://siamembers.siaonline.org/eweb/upload/imr/USSMRfactsheet.pdf>.

Le Livre blanc de Multimedia Intelligence⁴⁷ identifie six groupes de clients-clés pour les produits liés à la vidéosurveillance :

- Les milieux financiers et banquiers.
- Le secteur des transports.
- L'industrie.
- Le secteur du commerce au détail.
- Le secteur public.
- Le secteur de l'éducation.

Trois de ces secteurs, soit celui des transports, de l'éducation et du secteur public, sont très influencés par les gouvernements en termes de législations et de directives (normes, interopérabilité, etc.) ou en terme de financement. Selon cette firme, le marché résidentiel et de petites entités ne semble donc pas être une cible privilégiée de la vidéosurveillance.

La plupart des analystes considèrent que le marché global de la vidéosurveillance continuera lui aussi de croître au cours des prochaines années, mais les avis divergent quant au rythme anticipé de cette croissance.

Certaines organisations, comme ABI Research, proposent des prévisions très optimistes, estimant que le marché mondial de la vidéosurveillance devrait passer de 13,5 milliards de dollars US, son niveau en 2006, à 46 milliards de dollars en 2013, ce qui représente une hausse de 34 % par année sur sept ans. La firme IMS, quant à elle, mentionne des revenus globaux pour l'année 2007 de l'ordre de 7,25 milliards de dollars, ce qui est en deçà des estimations d'ABI Research, alors que la très respectée firme Freedonia parle d'une croissance annuelle de 6 % pour la vidéosurveillance⁴⁸. Face à ces données disparates, provenant probablement de définitions différentes du marché, on peut donc parler d'une fourchette de revenus pour l'année 2007 se situant entre 7,25 milliards de dollars (ÉU) et 14 milliards pour l'année 2007 à partir de ces deux sources, par exemple.

4.2.1 Moteurs du marché de la vidéosurveillance

Voici quelques moteurs du marché de la vidéosurveillance :

- Les suites du 11 septembre 2001 et la crainte inspirée par une nouvelle attaque terroriste (New-York, Londres, Madrid, Bali, Mumbai, etc.).

⁴⁷ Multimedia intelligence. 2008. *The Expanding World of IP Video Surveillance*.

⁴⁸ Institute of Management and Administration, Inc. Security's Director Report, Newsbrief, Février 2009, disponible à : https://www.ioma.com/?&IPAuth=&source=WW_200903&stype=WEB.

- Des événements tels que des fusillades dans des lieux publics, notamment dans des établissements d'éducation (Columbine, Virginia-Tech, Collège Dawson, etc.).
- Les hausses de la criminalité locale.
- Certaines avancées technologiques améliorant la performance des systèmes et/ou la réduction des coûts associés à leur installation ou à leur entretien.
- Un plus grand consentement de la population quant à l'installation de systèmes de vidéosurveillance dans les lieux publics.
- La possibilité d'utiliser les images recueillies lors de procédures judiciaires.
- La possibilité de faire converger la technologie de la vidéosurveillance avec d'autres technologies de contrôle d'accès (biométrie, par exemple).

4.2.2 Inhibiteurs du marché de la vidéosurveillance

Voici quelques inhibiteurs du marché de la vidéosurveillance :

- Les inquiétudes exprimées quant à la protection de la vie privée des individus.
- Les doutes sur l'efficacité de ces systèmes pour prévenir une attaque terroriste ou de type « Virginia-Tech ».
- La fiabilité des systèmes.
- La complexité d'installation et d'utilisation des systèmes (convivialité).
- Les coûts associés à leur entretien et à leur mise à niveau.
- L'absence de normes harmonisées au niveau de l'industrie.
- Une diminution des craintes liées à une attaque terroriste.
- Le manque de personnel qualifié.

De façon sectorielle, la firme ABI prévoit une importante croissance de la vidéosurveillance dans le marché des transports, avec des revenus de deux milliards de dollars (US), et dans celui du commerce au détail, qui devrait quant à lui générer des revenus de quatre milliards de dollars (US) en 2013⁴⁹.

4.2.3 Le marché de la vidéosurveillance IP et intelligente

La vidéosurveillance en est à un point tournant de son évolution, amorçant un passage vers le numérique et les infrastructures réseau IP⁵⁰. La flexibilité et l'extensibilité des systèmes IP, le fait que la plupart d'entre eux peuvent opérer sur du matériel non propriétaire, ainsi

⁴⁹ Video Surveillance Dollars Not Just for Security, ABI Research, 8 octobre 2008, <http://www.abiresearch.com/press/1257-Video+Surveillance+Dollars+Not+Just+for+Security>

⁵⁰ Russ Gazer. 2008. Special Report: Video Surveillance. SDM.

que les progrès technologiques au niveau des composantes, rendent ces systèmes plus intéressants pour les clients potentiels et tendent à en réduire les coûts.

Comme le mentionne le livre blanc de la firme Multimedia Intelligence, la croissance et les prévisions de croissance pour le marché de la vidéosurveillance IP sont très robustes. La sous-section des caméras IP, notamment, connaît une forte progression, ayant enregistré une hausse de 50 % des revenus en 2007, pour atteindre 500 millions de dollars mondialement⁵¹. Cette croissance est presque quatre fois supérieure à celle de l'ensemble des équipements de vidéosurveillance. Malgré tout, sur la base des revenus, les caméras IP ne représentent que 8 % du marché total des caméras de surveillance.

Le coût élevé des caméras IP, presque le double des caméras analogiques, constitue le principal frein à l'achat de celles-ci par les consommateurs⁵². Toutefois, selon certains experts, dans un horizon de trois à sept ans, les caméras IP devraient dominer le marché, entraînant l'essor de la vidéosurveillance « tout IP ». Les caméras mégapixel pourraient être le catalyseur de cette transition vers les technologies sur IP. Les avantages techniques en termes de qualité et de résolution d'image que procurent les caméras mégapixel en vidéosurveillance représentent une réelle motivation pour l'utilisateur. Axis est le plus grand manufacturier de caméras IP et Mobotix, le principal fabricant de caméras mégapixel.

L'avènement de la vidéosurveillance IP ne sonne pas le glas des systèmes de TVCF traditionnels utilisant des caméras analogiques. Les progrès techniques apportés par les manufacturiers aux enregistreurs numériques et enregistreurs numériques hybrides, tels que l'accès à distance, l'extensibilité et l'intégration d'analytique embarquée, les gardent compétitifs avec la vidéo sur réseau IP. Les deux types de technologies devraient cohabiter pendant quelques années et les systèmes hybrides devraient permettre une transition graduelle à la vidéosurveillance réseau.

Selon Frost & Sullivan⁵³, le secteur de l'éducation devrait s'imposer comme consommateur majeur de vidéosurveillance IP. La grande bande passante disponible sur les réseaux des institutions académiques leur permet de supporter la transmission vidéo. Ceci encourage le remplacement des infrastructures analogiques par des caméras IP. Toutefois, le commerce au détail demeure leader dans le déploiement des systèmes IP de vidéosurveillance.

La vidéosurveillance intelligente, quant à elle, constitue une industrie de niche qui en est encore à ses débuts. En ce qui concerne plus particulièrement le segment des logiciels de vidéosurveillance, ABI Research prévoit une forte croissance des revenus, de leur niveau

⁵¹ Multimedia Intelligence, *The Expanding World of IP Video Surveillance: Cameras, Storage, Technology and Semiconductors*, novembre 2008.

⁵² Selon IP Videomarket Info, seulement un acheteur sur cinq choisit des caméras IP.

⁵³ Frost & Sullivan, *World Video Surveillance Market- Investment Analysis*, juin 2008, <http://www.researchandmarkets.com/reports/612498>.

actuel à 245 millions de dollars, à plus de 900 millions de dollars en 2013⁵⁴. Cette prévision couvre tous les logiciels de vidéosurveillance, de la gestion vidéo à l'analytique. Sur la base des revenus, les deux plus gros joueurs mondiaux pour les logiciels de gestion vidéo sont Milestone et l'entreprise québécoise Genetec. Pour l'analytique vidéo, iomage Ltd. et ObjectVideo comptent parmi les compagnies les plus renommées⁵⁵.

Cependant, quelques analystes affichent une certaine déception quant à ce sous-secteur de la vidéosurveillance. Certaines barrières, quant à l'adoption plus généralisée de la vidéosurveillance intelligente, semblent continuer d'exister, notamment leur performance technique (par exemple, le nombre élevé de fausses alarmes), l'absence de standards au niveau de l'industrie, ce qui créerait de la confusion pour les clients potentiels et les coûts associés à la mise en place d'un système performant et efficace⁵⁶.

Dans cette optique, la vidéosurveillance intelligente continue de représenter un risque pour l'acheteur, étant donné une certaine confusion quant aux possibilités réelles des outils d'analytique vidéo disponibles sur le marché. Pour bien des applications, les capacités des systèmes d'analytique vidéo n'atteignent pas encore les attentes des utilisateurs. De plus, le prix de ces systèmes est encore élevé, ce qui les confine surtout à un marché haut de gamme, par exemple pour les réseaux de surveillance de grandes infrastructures, principalement publiques, ou critiques (par exemple, centrales énergétiques). Même dans ces secteurs, un analyste du marché estime que la majorité des déploiements de systèmes d'analytique vidéo en sont encore à la phase de projets pilotes⁵⁷.

Malgré ces difficultés, l'analytique vidéo s'avère très prometteuse pour améliorer l'efficacité de la surveillance par vidéo et de la recherche dans les séquences archivées. Actuellement, il existe chez les utilisateurs de vidéosurveillance un intérêt certain pour l'analytique vidéo, mais ceux-ci semblent attendre que cette technologie fasse ses preuves. Maintenant que certains traitements intelligents de la vidéo commencent à démontrer un rendement satisfaisant, on peut penser que la réelle croissance de ce marché reste à venir, mais celle-ci pourrait prendre quelques années à se matérialiser.

De plus, selon plusieurs analystes, de nouvelles applications moins liées à la sécurité (gestion des opérations, protection contre les poursuites, analyses du comportement des consommateurs, etc.) sont susceptibles de créer un regain d'intérêt pour ce type de systèmes et de contribuer à la croissance globale du secteur à moyen et plus long termes.

⁵⁴ Strong growth for video surveillance software, Security Info Watch, 11 juin 2008, <http://www.securityinfowatch.com/online/Research--Studies-and-Whitepapers/15921SIW321>.

⁵⁵ John Honovich, *How U.S. IP video companies fit into the world market*, 8 mars 2009, SecurityInfoWatch.com disponible à : <http://www.securityinfowatch.com/CCTV+%2526+Surveillance/1309661>.

⁵⁶ John Honovich, *Video Surveillance Market Size & Forecast Reference Guide*, IP Video Market Info, 24 janvier 2009, disponible à : http://ipvideomarket.info/report/video_surveillance_market_size_forecast.

⁵⁷ Simon Harris de IMS Research, cité par Geoff Kohl dans SecurityInfoWatch.com, 11 mars 2009, *Where video analytics is today*.

4.2.4 Les joueurs

La vidéosurveillance constitue un marché très fragmenté où plusieurs joueurs se partagent la clientèle. Il existe des joueurs dominants dans certains segments, tels qu'Axis pour les caméras IP, Pelco pour les caméras analogiques et Genetec pour les logiciels de gestion vidéo, mais beaucoup de concurrents s'approprient de petites parts du marché. L'industrie est caractérisée par d'inévitables partenariats entre les manufacturiers d'équipements, les développeurs de logiciels de gestion vidéo et d'analytique, afin d'assurer une compatibilité entre les différentes composantes d'un système de vidéosurveillance.

Il est intéressant de noter l'entrée en scène, dans le marché de la vidéosurveillance, de joueurs plus traditionnellement associés aux TI, tels que Cisco, IBM et EMC⁵⁸. Selon MMI, ceci tend à modifier l'environnement d'affaires des firmes plus « traditionnelles » de vidéosurveillance, telles qu'Axis Communications. Cela indique également un certain intérêt de la part de ces firmes envers les marchés de vidéosurveillance et la convergence anticipée entre sécurité physique et sécurité logique.

Le classement des 50 plus importantes firmes de sécurité de l'année 2008 effectué par Asmag⁵⁹, sur la base des revenus, indique que 30 d'entre elles ont pour principale force la vidéosurveillance. Il est intéressant de noter qu'une seule entreprise canadienne, March Networks, s'y trouve et qu'elle se situe au 21^e rang du classement⁶⁰.

4.2.5 L'impact de la récession sur le marché

Il est actuellement très difficile de cerner les impacts qu'aura la crise financière sur le marché de la sécurité et sur celui de la vidéosurveillance. Les avis sont très partagés à ce sujet.

Pour plusieurs firmes de consultants, le marché de la sécurité est à l'épreuve de la récession dans la mesure où une part des activités de ce marché est déterminée par la demande publique et gouvernementale. De plus, certains voient une corrélation entre les périodes de crises économiques et la hausse de la criminalité, ce qui pourrait se traduire par des ventes accrues dans les systèmes de sécurité, y compris ceux de vidéosurveillance. Par ailleurs, les systèmes de vidéosurveillance intelligente pourraient représenter une alternative intéressante aux dispositifs plus classiques, puisqu'ils nécessitent moins de personnel. C'est ce que tend à souligner un article paru dans le Boston Globe au mois de février 2009⁶¹ et la plupart des firmes de consultants qui continuent d'envisager une croissance dans ces marchés.

⁵⁸ Frost & Sullivan 2008, op. cit.

⁵⁹ Fabrication uniquement, excluant donc l'installation, la distribution et la revente.

⁶⁰ Asmag.com, Security Top 50, 2009.

⁶¹ Kirsner, Scott. Surveillance gest intelligent. *Security Firms see Growth as the Downturn Worsens*, 8 février 2009.

Toutefois, d'autres craignent que le marché de la sécurité et celui de la vidéosurveillance ne soient pas à l'abri de baisses dans les revenus. L'édition 2009 de l'Industry Forecast de SDM portant sur la sécurité électronique affiche très clairement que, pour la première fois depuis que l'organisme fait cet exercice, les répondants au sondage annuel anticipent une baisse de leurs revenus totaux de l'ordre de 7,8 % en 2009. John Honovich, d'IP Video Market Info, prédit également une baisse substantielle de la croissance pour la vidéosurveillance IP entre 2008 et 2009 par rapport aux prévisions de 2008. Il souligne d'ailleurs le fait que la plupart des études de marché prévoyant des hausses appréciables du volume d'affaires ont été publiées avant les dépôts des rapports financiers pour le quatrième trimestre. Il enjoint donc ses lecteurs à faire preuve de prudence, car, dans le contexte économique actuel, les projections deviennent très hasardeuses.

Severin Sorensen de la firme Sikyur LLC tend également à prescrire la prudence, mentionnant que si l'entreprise dispose d'une technologie de rupture permettant de faire économiser à son client des sommes d'argent importantes, alors le marché lui est favorable. Par contre, pour les projets requérant de lourds investissements, les pronostics sont nettement moins bons, compte tenu des difficultés économiques actuelles⁶². Il met également un bémol sur le côté « à l'épreuve de la récession » des marchés publics : ces derniers ne sont pas uniquement fédéraux, ils sont également provinciaux et municipaux. Or, comme le soulève le Center on Budget and Policy Priorities⁶³, les États fédérés américains connaissent actuellement une importante crise financière directement tributaire de la crise économique globale. Cette situation risque de ralentir plusieurs projets qui devaient être mis sur les rails au courant de l'année et la situation serait sensiblement la même au niveau municipal. Cependant, le plan de relance proposé par le président Obama et adopté par le Congrès comprend des dispositions en matière de sécurité locale pouvant mener à des occasions d'affaires de l'ordre de 4,5 milliards de dollars US⁶⁴, ce qui pourra aider à redresser, du moins partiellement, la situation. Il reste à attendre de voir comment ces fonds seront dépensés.

Au Canada, le Plan d'action économique ne fait pas véritablement mention de la question de la sécurité intérieure⁶⁵. Une annonce en lien avec l'amélioration de la sécurité dans les aéroports du pays y est faite, mais c'est tout⁶⁶. Il est donc très difficile de jauger l'impact de la crise sur le marché canadien, dans la mesure où les données sur ce dernier sont difficiles à obtenir et ne sont souvent pas récentes. Même si sous plusieurs aspects, le Canada et le

⁶² Sorensen, Severin. *Recession Impacting Security Projects*. IPVideoMarket Info, 10 février 2009, disponible à http://ipvideomarket.info/report/recession_impacting_security_projects.

⁶³ Center on Budget and Policy Priorities, *State Budget Troubles Worsen*, By [Elizabeth McNichol](#) and [Iris J. Lay](#), 13 mars 2009, disponible à <http://www.cbpp.org/files/9-8-08sfp.pdf>.

⁶⁴ William Welsh, *Stimulus to generate \$4.5B state and local tech spending*, Washington Technology, 13 février 2009, disponible à : <http://www.washingtontechnology.com/Articles/2009/02/13/Stimulus-to-generate-new-state-and-local-tech-spending.aspx>.

⁶⁵ Canada, ministère des Finances, *Le plan d'action économique du Canada. Le budget de 2009*, 27 janvier 2009.

⁶⁶ Gouvernement du Canada. 23 janvier 2009. *Le gouvernement du Canada investit dans la sécurité aéroportuaire au Canada*. Communiqué.

Québec semblent actuellement mieux résister à la crise que d'autres joueurs nationaux ou provinciaux, les déficits budgétaires annoncés sont peut-être susceptibles de mettre certains projets d'envergure sur la glace. Il faut mentionner que rien n'a été annoncé à cet effet jusqu'à ce jour.

Au niveau du secteur privé, plusieurs notent déjà un resserrement des dépenses en sécurité des entreprises et un recentrage des priorités en ce domaine sur l'entretien et l'opération de systèmes déjà en place, plutôt que sur l'installation de nouveaux systèmes⁶⁷.

4.3 L'offre et la demande en vidéosurveillance IP et intelligente au Québec

Peu de données publiques sur le secteur spécifique de la vidéosurveillance au Québec sont disponibles et celles-ci datent parfois de quelques années. Pour dépeindre le secteur de la vidéosurveillance IP et intelligente au Québec, une étude exhaustive auprès des différents joueurs du marché dépassait le cadre de ce rapport. Quelques représentants du marché - développeurs, intégrateurs et installateurs, grands utilisateurs de vidéosurveillance numérique - ont donc été sélectionnés. Ils ont été questionnés sur les besoins des clients, les services offerts, les produits disponibles. Leurs commentaires sur l'état actuel de l'industrie québécoise de la vidéosurveillance et les débouchés pour l'analytique vidéo ont été colligés.

À partir des témoignages recueillis et, en perspective avec les analyses du marché mondial de la vidéosurveillance disponibles publiquement, cette section dresse un portrait des tendances de l'offre et de la demande québécoise en matière de vidéosurveillance numérique. Les entreprises et centres de recherche québécois offrant une expertise particulière en matière de vidéosurveillance numérique et intelligente y sont identifiés et une liste des principaux joueurs, québécois et internationaux, dans ce marché est disponible aux Annexes 2, 3 et 4. Quelques recommandations sur le positionnement du marché québécois dans ce secteur sont aussi avancées.

4.3.1 La demande

Selon les experts interrogés, il existe au Québec, à l'instar des autres pays industrialisés, une demande forte pour les systèmes de vidéosurveillance. Ceux-ci font partie des équipements nécessaires de sécurité. La vidéosurveillance numérique IP commence à s'implanter, mais surtout dans le marché haut de gamme. Les larges réseaux de vidéosurveillance IP se retrouvent notamment dans les secteurs public et parapublic, les transports, les grandes chaînes de commerce au détail, les casinos et les universités. Les

⁶⁷ Sorensen, op.cit.

commerces de petite et moyenne tailles tardent à passer à la vidéosurveillance IP, notamment en raison des coûts plus élevés des équipements.

En 2003-2004, la Commission québécoise d'accès à l'information a tenu une consultation publique sur l'utilisation de la vidéosurveillance par les organismes publics dans les lieux publics⁶⁸. Déjà à cette époque, on y dévoilait que la majeure partie des organismes publics et parapublics de la province (incluant les municipalités) utilisaient des systèmes de vidéosurveillance, ce qui représentait en 2003-2004 plus de 5 000 caméras. De plus, pratiquement toutes les nouvelles constructions publiques au Québec sont équipées des câblages nécessaires à l'installation d'un système de vidéosurveillance, ce qui tend à indiquer que l'usage de ce type d'équipement est désormais entré dans les pratiques des organisations.

Dans le secteur des transports, Aéroports de Montréal (ADM) et la Société de transport de Montréal (STM) ont été cités en exemple à la section 2.4 pour l'utilisation de vidéosurveillance. Ils représentent des réseaux de plusieurs centaines de caméras. À la STM, particulièrement, le virage IP a été opéré. De plus, le milieu des transports commence à intégrer des produits d'analytique, au moins à titre de projet pilote.

Une étude réalisée conjointement par PriceWaterhouseCoopers et par le Conseil canadien des commerçants au détail révélait que 90 % des répondants à un sondage sur les mesures de sécurité prises contre le vol, utilisaient des systèmes de vidéosurveillance⁶⁹. Il ne serait pas étonnant que, plus spécifiquement au Québec, on retrouve aussi la vidéosurveillance dans une forte proportion des commerces. Le cas des dépanneurs Couche-Tard a déjà été cité en exemple à la section 2.3, pour son utilisation d'analytique vidéo.

Les universités québécoises doivent assurer la sécurité de larges campus, comprenant plusieurs bâtiments et stationnements, parfois très dispersés géographiquement. La vidéosurveillance y est implantée depuis plusieurs années. Avec la nécessité de renouveler les équipements brisés ou désuets, les institutions universitaires migrent de plus en plus vers la vidéosurveillance IP. Par exemple, à l'Université McGill, le réseau de vidéosurveillance est déjà hybride, comprenant caméras analogiques et IP, et enregistreurs numériques. Les solutions d'enregistrement sur réseau y sont maintenant considérées.

Dans le rapport final, résultant de la consultation publique de la commission d'accès à l'information, tenue en 2004⁷⁰, le commissaire relevait que l'usage des systèmes de vidéosurveillance par l'entreprise privée est insuffisamment documenté au Québec. Ce marché, selon les experts consultés pour ce rapport, est principalement constitué de PME. Celles-ci ont des moyens modestes à allouer à la sécurité. Les systèmes de

⁶⁸ Commission d'accès à l'information du Québec. Consultation publique. *L'utilisation de caméras de surveillance par les organismes publics dans les lieux publics*. Bilan, avril 2004.

⁶⁹ Canada Newswire. Juin 2008. *Survey shows Canadian Retailers are Taking Necessary Actions to Combat Theft : Retail Council of Canada*, PriceWaterhouseCoopers.

⁷⁰ Commission d'accès à l'information du Québec, op.cit.

vidéosurveillance implantés dans ces entreprises comportent typiquement moins de 50 caméras. Dans la plupart des cas, cette clientèle ne connaît pas l'existence de l'analytique vidéo. Toutefois, elle apprécie des fonctionnalités, comme le suivi automatisé d'objet à l'aide de caméras PTZ.

Pour l'ensemble des secteurs, les experts consultés ont émis différents commentaires pour caractériser la demande québécoise pour la vidéosurveillance. Le marché québécois de la vidéosurveillance serait moins mature que les marchés américains ou européens. Les entreprises et organismes publics sont très souvent en mode réactif pour le déploiement de systèmes de sécurité. Ils ne se croient pas à risque jusqu'à ce que survienne un événement grave.

Au Québec, les clients privilégient surtout des systèmes déjà faits, contrairement aux utilisateurs européens qui se font plus fréquemment développer des solutions sur mesure, par exemple. Les systèmes propriétaires sont plus populaires au Québec que les systèmes ouverts, qui sont beaucoup plus prisés en Europe.

Les utilisateurs québécois, tout comme à ceux des autres pays, cherchent à diminuer le personnel affecté à la surveillance. De plus, dans plusieurs cas, ils souhaitent passer d'une surveillance réactive à une surveillance préventive et obtenir des outils plus performants pour la recherche dans les archives vidéo. L'analytique vidéo peut apporter certaines solutions à ces problèmes, mais les utilisateurs ne connaissent pas encore bien les possibilités et limites de cette technologie. L'analytique fait surtout une percée dans les grandes entreprises ou infrastructures, mais pas encore dans les systèmes destinés aux PME.

Le marché québécois comporte des besoins particuliers en matière de vidéosurveillance. Les conditions météorologiques extrêmes (froid et chaleur, neige, etc.) que connaît le Québec, peuvent affecter le fonctionnement des composantes matérielles de vidéosurveillance. De plus, les variations du climat représentent un défi supplémentaire pour les algorithmes d'analytique vidéo. Finalement, la société québécoise est la seule en Amérique du Nord à rechercher des logiciels de vidéosurveillance en français.

4.3.2 L'offre

L'industrie se divise principalement entre les manufacturiers, les distributeurs, les revendeurs-installateurs, les intégrateurs-installateurs et les développeurs de logiciels de gestion vidéo ou d'analytique. Les revendeurs-installateurs vendent des solutions complètes qu'ils achètent aux distributeurs et en font l'installation chez le client pour une solution clé en main. Les intégrateurs-installateurs, quant à eux, montent eux-mêmes les ordinateurs et serveurs pour composer un système adapté aux besoins du client.

Les plus gros distributeurs de produits de vidéosurveillance pour le Canada et le Québec sont ADI-Burtek et Tri-Ed. La plupart des produits vendus sur le marché québécois proviennent de manufacturiers étrangers, surtout américains. On note que les caméras et logiciels vidéo chinois et coréens font leur entrée sur le marché canadien depuis environ un an. Pour l'instant, ces produits sont rudimentaires et n'atteignent pas le niveau de qualité et de fonctionnalités des produits occidentaux, mais ils pourraient se développer.

Il existe plusieurs revendeurs-installateurs et intégrateurs-installateurs au Québec. Il s'agit souvent de toutes petites entreprises. Certaines grandes entreprises de sécurité et d'alarme, telles que ADT et Protectron, offrent des services d'installations de systèmes de vidéosurveillance, mais ce n'est pas leur spécialité. Très peu d'intégrateurs au Québec sont spécialisés dans la vidéosurveillance IP. Parmi eux, Claridion et SGPTI ont été rencontrés pour cette étude de veille. Dans le cadre de ce rapport, les revendeurs-installateurs et les intégrateurs-installateurs n'ont pas été recensés. Toutefois, ceux qui ont été mentionnés par les experts interviewés sont inclus à la liste des entreprises à l'Annexe 3.

Dans la classe des concepteurs de logiciels, Genetec représente un fleuron de l'industrie québécoise. Il s'agit de l'un des deux plus gros développeurs de logiciels de gestion vidéo au niveau mondial. En 2008, le journal *Les Affaires* rapportait que le chiffre d'affaires de l'entreprise avait augmenté de 900 % en cinq ans⁷¹. Son système le plus sophistiqué peut gérer jusqu'à 250 000 caméras grâce à un réseau IP. Le logiciel de Genetec intègre des fonctions d'analytique vidéo développées par des tiers.

VideoWave Networks et Organix IT sont deux autres exemples d'entreprises québécoises développant des logiciels de gestion vidéo intégrant des fonctionnalités intelligentes. VideoWave Networks se spécialise dans les logiciels pour la gestion de caméras PTZ, et Organix IT, en partenariat avec ISS Technology, offre un logiciel de gestion vidéo à architecture ouverte.

Dans le segment des caméras, ImmerVision développe des logiciels et des optiques panoramiques qui permettent la captation, le traitement et la visualisation de photos et de vidéos à 360 degrés. L'entreprise Obzerv, quant à elle, a mis sur le marché une technologie novatrice de système de vision nocturne pour la surveillance.

De façon globale, il existe plusieurs fournisseurs dans le domaine de la vidéosurveillance au Québec, mais en général, les entreprises sont assez petites (moins de dix employés). La plupart d'entre elles offrent des services d'intégration et d'installation. Il existe donc une forte concurrence dans ce secteur. Toutefois, aux dires des experts interviewés, il n'existe pas encore une masse critique de fournisseurs spécialisés en vidéosurveillance IP. Les entreprises traditionnelles de sécurité physique ne possèdent pas nécessairement l'expertise en TI requise pour l'installation des systèmes sur réseaux IP. De l'opinion de certains experts consultés, la demande surpasse l'offre en matière de vidéosurveillance numérique.

⁷¹ *Les Affaires*, *Genetec veut consolider ses acquis*, 5 juillet 2008, p. 24.

L'offre de produits, quant à elle, est principalement étrangère. Mis à part Genetec, il existe peu de développeurs de solutions de vidéosurveillance numérique au Québec. Pourtant, le Québec compte une forte expertise dans le domaine de la vision et de l'analyse d'images. Quelques centres de recherche, notamment dans les universités Laval, McGill, Concordia et Polytechnique, et ainsi qu'au CRIM, se spécialisent dans l'analytique vidéo et pourraient transférer des connaissances et des technologies dans ce domaine aux entreprises québécoises.

4.3.3 Recommandations pour le marché québécois

Le marché de la sécurité, et particulièrement le marché de la vidéosurveillance, est en pleine croissance à l'échelle de la planète et offre d'intéressantes occasions d'affaires. Une entreprise n'a pas besoin d'être très grande pour intégrer ce marché, déjà très fragmenté. La transition à la vidéosurveillance sur réseau IP, ainsi que l'analytique vidéo, ouvrent de nouveaux créneaux de développement.

En raison de la forte expertise en TI présente au Québec, les entreprises et universités québécoises sont bien positionnées pour profiter des opportunités de développement technologique et commercial qu'offre l'émergence de la vidéosurveillance intelligente.

Afin de favoriser le positionnement des entreprises québécoises dans ce secteur, quelques recommandations peuvent être formulées.

- Il serait bénéfique que la communauté des TI se rapproche d'avantage de l'industrie de la vidéosurveillance avec la venue des caméras IP et de la surveillance réseau. La migration des systèmes de vidéosurveillance sur réseaux IP soulève plusieurs problèmes de TI, dont :
 - l'utilisation optimale de réseaux (la transmission vidéo consomme beaucoup de bande passante) ;
 - la création d'interfaces et de composantes logicielles pour la gestion intelligente de la vidéo de surveillance sur intranet ou Internet ;
 - la fouille efficace de larges banques de données, possiblement vidéo, sur réseau ;
 - l'intégration automatique de la vidéosurveillance avec les systèmes géomatiques, GPS et autres systèmes de sécurité.
- Les développeurs québécois devraient prendre le virage intelligent amorcé en vidéosurveillance. Ils auraient avantage à se positionner dans ce secteur de niche et à tirer profit de l'expertise déjà existante en analytique vidéo dans les universités et centres de recherche québécois. Les nouvelles applications de la vidéosurveillance intelligente, telles que l'analyse des comportements des consommateurs et la gestion des opérations d'entreprises, semblent des secteurs prometteurs commercialement, car elles démontrent un retour sur l'investissement du consommateur.

- Les utilisateurs ne devraient pas miser que sur les composantes matérielles, mais aussi investir dans l'intelligence des systèmes. Il faudra notamment prévoir la gestion des masses de données vidéo et développer des techniques pour détecter en temps réel des anomalies, indexer le contenu vidéo et créer des sommaires vidéo pour la recherche après le fait.
- Il serait souhaitable, par exemple, d'assurer une concertation des développeurs et fournisseurs par la création d'un consortium permettant de rassembler les intervenants en vidéosurveillance IP.
- Les développeurs de logiciels de gestion vidéo devront porter attention aux efforts de standardisation entrepris pour la vidéosurveillance IP et y participer.
- Afin d'assurer une offre de service suffisante en vidéosurveillance sur réseaux IP par des fournisseurs compétents, il est nécessaire de former les intégrateurs-installateurs pour leur fournir les compétences en TI, ainsi que les connaissances sur la sécurité physique que cette technologie requiert.
- De la même façon, il serait souhaitable que les intégrateurs-installateurs reçoivent une formation sur les produits d'analytique vidéo. De plus, afin d'augmenter l'adoption de ces technologies, les développeurs devraient rendre la configuration et l'installation de leurs logiciels aussi conviviales que possible pour les intégrateurs et installateurs.
- Il y a un besoin pour des « super-intégrateurs » capables de coordonner l'élaboration et la mise en place des différents systèmes de sécurité, de façon intégrée, pour la commande centralisée d'exploitation de grandes installations de sécurité. Ceci faciliterait la vie des clients qui doivent interagir avec plusieurs intégrateurs pour monter un système unifié de surveillance.
- Il est important de faire connaître à la clientèle (gouvernements, transports, éducation, etc.) les avantages et les inconvénients de vidéo IP et les possibilités, sans exagération, de l'analytique vidéo.
- Le choix de la vidéosurveillance IP devrait être privilégié pour les grands déploiements ou lorsque l'infrastructure réseau est déjà disponible.
- Les utilisateurs devraient investir dans des systèmes de caméras à grands angles ou panoramiques et les caméras mégapixel, plutôt que sur un grand nombre de caméras standard. Le désavantage cependant est qu'un bris d'une caméra panoramique a plus de conséquences que celui de quelques caméras sur un gros réseau.
- Le Québec doit offrir plus d'aide financière pour la commercialisation des produits développés et l'expansion des entreprises, car les fonds sont surtout alloués pour la recherche et le développement. Les capitaux de risque se retirent souvent trop hâtivement des entreprises.

5. ENJEUX

Malgré leur adoption grandissante, les technologies de vidéosurveillance soulèvent certains enjeux et sont confrontées à d'importantes résistances. Cette section traite de trois problèmes reliés à la vidéosurveillance et qui pourraient avoir un impact majeur sur son implantation et sur son développement.

5.1 Protection de la vie privée

Le vaste recours à la vidéosurveillance, dans les lieux publics et privés, soulève plusieurs préoccupations chez les groupes défendant le respect de la vie privée. Avec des caméras pointées un peu partout dans les rues, dans les parcs, dans les édifices, dans les commerces, possiblement chez leur employeur, plusieurs gens craignent une mauvaise utilisation de cette vidéo et des informations personnelles qu'elle contient. Dans les mains des pouvoirs publics et des forces de l'ordre, il ne faudrait pas que la vidéosurveillance permette de dresser le profil des gens filmés ou qu'elle soit utilisée à des fins futiles ou discriminatoires.

Le Commissariat à la protection de la vie privée du Canada a formulé des lignes directrices, afin de mieux définir et encadrer l'utilisation de cet outil de surveillance, tant par les autorités et forces policières dans les lieux publics⁷², que par les organisations du secteur privé⁷³. La surveillance vidéo est assujettie à la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)*. Toutefois, les dispositions du Code criminel relatives à l'enregistrement de communications privées s'appliquent à l'utilisation d'une caméra qui capte les sons.

« Les lignes directrices sont formulées sous forme de principes et permettent d'évaluer s'il est nécessaire d'avoir recours à la surveillance vidéo et, le cas échéant, de veiller à ce qu'elle soit effectuée de façon à brimer le moins possible la vie privée des gens ». ⁷⁴ De façon générale, il faut justifier la nécessité d'utiliser des caméras de surveillance et, si possible, privilégier d'autres moyens. Par exemple, un magasin pourrait décider de mettre sous clé les articles de grande valeur, plutôt que de recourir à une surveillance vidéo en continu. La vidéosurveillance doit donc être utilisée pour traiter un problème réel, spécifique et important. De plus, l'espace couvert par les caméras, ainsi que le temps de surveillance doivent être réduits au strict nécessaire. Il est entendu que les caméras sont

⁷² Lignes directrices du Commissariat à la protection de la vie privée du Canada concernant le recours, par les forces policières et les autorités chargées de l'application de la loi, à la surveillance vidéo dans les lieux publics, 2006, http://www.privcom.gc.ca/information/guide/vs_060301_f.asp.

⁷³ Lignes directrices sur la surveillance vidéo au moyen d'appareils non dissimulés dans le secteur privé, 2008, http://www.privcom.gc.ca/information/guide/2008/gl_vs_080306_f.asp.

⁷⁴ Lignes directrices du Commissariat à la protection de la vie privée du Canada concernant le recours, par les forces policières et les autorités chargées de l'application de la loi, à la surveillance vidéo dans les lieux publics, 2006, op.cit.

proscrites des endroits où les gens s'attendent habituellement à conserver une intimité (toilettes, vestiaires, salles d'essayage, douches, etc.). Le public doit être informé de la présence de caméras de surveillance et les personnes filmées ont droit d'avoir accès à leurs renseignements personnels.

Dans le secteur public, comme dans le secteur privé, les organisations ayant recours à la surveillance vidéo devraient élaborer une politique pour encadrer son usage, définir précisément les objectifs de la surveillance et les emplacements du matériel, contrôler l'accès à la vidéo captée, protéger les renseignements personnels et limiter le temps d'archivage des séquences vidéo, sauf, évidemment, pour celles requises pour une enquête.

Ces lignes directrices ne visent pas à entraver le pouvoir des corps policiers à mener des enquêtes. De plus, dans le secteur privé, elles ne s'appliquent qu'aux appareils non dissimulés et ne couvrent pas l'équipement dissimulé qui pourrait, par exemple, être utilisé pour les enquêtes menées par des compagnies d'assurance.

En ce qui concerne l'utilisation de vidéosurveillance par les employeurs dans leur entreprise, il existe encore peu de jurisprudence pour orienter la pratique. Dans cette situation, deux droits s'affrontent : le droit de l'employé à la protection de sa vie privée sur les lieux de son travail et celui de l'employeur de protéger son entreprise. Encore une fois, deux principes devraient guider l'installation de caméras en milieu de travail, soit la preuve de la nécessité d'une surveillance vidéo pour la protection des lieux, du personnel et des installations sous la responsabilité de l'employeur et le souci de minimiser l'étendue de l'intrusion dans la vie privée de l'employé. Par exemple, il pourra être acceptable de retrouver des caméras pour contrôler les accès à l'édifice ou à des aires sensibles. Toutefois, il est excessif d'orienter directement une caméra sur le poste de travail d'un employé et de le filmer pendant tout son quart de travail. Un employeur ne peut filmer un employé que s'il a un doute raisonnable qu'il a commis ou qu'il s'apprête à commettre un délit. Le système de surveillance vidéo ne peut toutefois être utilisé pour surveiller la productivité des employés ou évaluer la qualité de leur travail. Fait important à noter, la responsabilité de l'employeur de faire un usage mesuré de la vidéosurveillance s'étend à toutes les personnes amenées à visionner la vidéo provenant de caméras de surveillance en entreprise, même les sous-contractants engagés à cet effet.

L'essor de la vidéosurveillance dans les lieux publics, dans les entreprises et même dans les résidences privées, soulève la question de la protection des renseignements personnels des gens filmés. Bien que les populations acceptent de plus en plus la présence de caméras pour des raisons de sécurité, la protection de la vie privée demeure tout de même une préoccupation exprimée lors de nouveaux déploiements de caméras de surveillance, surtout dans les aires publiques.

Certains soutiennent que l'analytique vidéo pourrait contribuer à protéger les données personnelles captées sur vidéo. Le traitement automatique des images permet, par exemple, de masquer les visages ou les objets non pertinents sur la vidéo préalablement à sa

transmission pour visionnement. De plus, la détection d'individus ou de comportements suspects par un ordinateur pourrait diminuer le risque de profilage, c'est-à-dire de surveillance basée sur la couleur, la race ou le groupe d'appartenance des personnes filmées. Toutefois, l'usage de la vidéosurveillance intelligente pour des fins autres que la sécurité, telle que l'analyse des comportements de consommation, peut remettre en question le principe de nécessité de la vidéosurveillance.

5.2 Efficacité de la vidéosurveillance pour la réduction de la criminalité

Les systèmes de vidéosurveillance sont déployés dans la plupart des grandes villes du monde. Ces systèmes permettent-ils de diminuer la criminalité et d'aider à élucider plus de crimes? Plusieurs études ont analysé l'efficacité des systèmes de vidéosurveillance. Les résultats de celles-ci diffèrent grandement, certaines révélant de très forts taux de réduction de crimes, tandis que d'autres constatent une faible incidence sur la criminalité suite à l'installation de caméras de surveillance.

Mesurer les impacts des systèmes de vidéosurveillance s'avère complexe, car plusieurs facteurs peuvent expliquer la hausse ou la baisse de la criminalité. Toute variation doit être mise en contexte avec la tendance générale de la criminalité, son possible déplacement à d'autres régions et l'effet combiné de plusieurs mesures de sécurité, telle que le renforcement des patrouilles policières ou l'amélioration de l'éclairage d'une région.

Suite à une revue des études publiées sur le sujet, Dee et Velastin [8] rapportent qu'il n'existe pas vraiment de preuves tangibles que la vidéosurveillance permet de réduire la criminalité. L'ACLU Technology and Liberty Program affirme que, pour évaluer l'efficacité de la vidéosurveillance, il est plus fiable de faire la méta-analyse de plusieurs études, afin d'obtenir des données statistiquement robustes, que de considérer une étude individuelle⁷⁵. Des études de ce type menées pour le compte du Home Office de Grande-Bretagne constatent peu d'impact de la surveillance vidéo sur la réduction de la criminalité⁷⁶ et ⁷⁷.

De même, aux États-Unis, une étude récente sur le programme de vidéosurveillance de la ville de San Francisco, dans les quartiers aux prises avec une forte criminalité, a démontré que l'installation de caméras de surveillance n'a pas réduit le nombre d'homicides et de crimes violents. Par contre, elle a fait chuter les délits mineurs, tels que les vols à la tire, les cambriolages et le vandalisme. Par ailleurs, des failles technologiques et organisationnelles

⁷⁵ Noam Biale, ACLU Technology and Liberty Program, *What Criminologists and Others Studying Cameras Have Found*, <http://www.youarebeingwatched.us/about/182/>.

⁷⁶ Welsh, B. and Farrington, D., *Crime Prevention Effects of Closed Circuit Television: A Systematic Review* (2002), Home Office Research, Development and Statistics Directorate. Cité dans <http://www.youarebeingwatched.us/about/182/#footnote10>.

⁷⁷ Gill and Spriggs, *Assessing the Impact of CCTV*. (2005) Home Office Study. Cité dans <http://www.youarebeingwatched.us/about/182/#footnote10>.

dans l'opération du système de vidéosurveillance sont identifiées. Fait à noter, dans ce programme, les policiers ne peuvent utiliser les images vidéo que comme outils d'enquête lorsqu'un crime est commis, afin de prévenir les atteintes à la vie privée que pourraient engendrer la surveillance en temps réel. Dans ce contexte, la présence de caméras ne semble avoir aucun effet dissuasif pour les crimes violents, souvent commis irrationnellement, mais s'avère efficace pour décourager les larcins. Il s'agit de l'un des rapports les plus complets sur la surveillance publique aux États-Unis⁷⁸.

Ainsi, il n'y a pas de preuves claires que l'installation de caméras de surveillance puisse réduire la criminalité. Dans certains cas, les systèmes de vidéosurveillance ont semblé avoir un impact sur des crimes prémédités, mais pas sur les crimes spontanés. La présence de caméras semblait cependant efficace sur la diminution de vols de voitures dans des stationnements.

En ce qui concerne la résolution des crimes, un article de l'Actualité rapportait qu'à Londres, capitale la plus surveillée par caméra, seulement 3 % des vols sont élucidés grâce au système de vidéosurveillance⁷⁹. Les policiers trouveraient trop fastidieux de chercher dans les quantités d'images vidéo archivées pour leurs enquêtes. Pourtant, le système de vidéosurveillance londonien a connu certains succès, lorsque les images vidéo ont permis d'identifier les terroristes qui avaient tenté de faire exploser des bombes dans le métro, en 2005.

Les conclusions de ces études apportent un sérieux bémol sur l'efficacité de la vidéosurveillance pour lutter contre la criminalité. Néanmoins, elles ne permettent pas de conclure à l'inutilité des systèmes de surveillance vidéo. Les limites techniques de ces systèmes, les conditions dans lesquelles ils sont déployés, ainsi que le mode d'utilisation influent grandement sur les résultats qu'ils permettent d'obtenir. Par exemple, pour être efficaces, ces systèmes doivent faire partie d'un ensemble de mesures de sécurité et être déployés avec des objectifs opérationnels précis.

À elles seules, les caméras ne semblent pas constituer un moyen de dissuasion efficace pour beaucoup de crimes. La surveillance vidéo passive, après le fait, ne permet donc pas de prévenir les délits. Par contre, la surveillance active, en continu, soulève des problèmes de respect de la vie privée. Il est donc imaginable que des algorithmes de traitement intelligent capables d'actionner des alarmes efficacement, pourraient permettre une surveillance acceptable en temps réel aidant à intervenir lors de la perpétration d'actes criminels. De plus, l'analytique vidéo pourrait contribuer à élucider plus de crimes, si elle fournit des méthodes efficaces de recherche dans les séquences vidéo archivées. L'amélioration de la qualité des images vidéo apportera sans doute de grands progrès pour l'identification des suspects.

⁷⁸ Security Info Watch, *Study gives split verdict on crime cameras*, 8 mars 2009, <http://www.securityinfowatch.com/root+level/1309228>.

⁷⁹ Schaëffner, Yves, « *Big Brother* » est aveugle, L'Actualité, 15 octobre 2008.

5.3 Standards pour la vidéo IP

Maintenant que la vidéosurveillance sur réseau IP connaît un essor, les manufacturiers travaillent à ébaucher un standard régissant la communication entre les caméras IP et les logiciels de gestion vidéo. Actuellement, chaque fabricant doit développer les interfaces permettant à leurs caméras de se connecter et d'échanger de l'information avec les logiciels de gestion vidéo. Cette activité est coûteuse en temps et en argent. L'adoption d'un standard, en favorisant l'interopérabilité des différents produits disponibles, permettra au marché de la vidéosurveillance IP de se développer plus rapidement, diminuant les coûts pour les manufacturiers et les clients.

Alors, que le SIA Standards Committee⁸⁰ travaille depuis quelques temps à définir un standard pour la vidéosurveillance IP, deux groupes insatisfaits de la lenteur du processus ont lancé leurs propres initiatives. Il s'agit de la PSIA (Physical Security Interoperability Alliance), menée par Cisco Systems, DVTel, General Electric, Honeywell, IQinVision, Panasonic, Pelco et Verint, et du ONVIF (Open Network Video Interface Forum), mené par Axis, Bosch et Sony⁸¹.

Sans l'avouer, ces deux groupes se mènent une lutte pour développer et imposer leur standard, afin d'assurer leur avantage concurrentiel dans le marché. Axis, Bosch et Sony détiennent déjà plus de 50 % des parts du marché des caméras. Ces entreprises ont donc peu d'avantages à tirer de l'éclosion d'un standard, puisqu'en tant que leaders, leurs produits sont déjà supportés par la plupart des systèmes de gestion vidéo. Elles ont plutôt intérêt à contrôler ou retarder le développement d'un standard qui pourrait faciliter l'accès au marché de leurs compétiteurs. Par contre, les manufacturiers soutenant le PSIA détiennent de petites parts du marché des caméras. C'est pourquoi ils pressent la mise en place d'un standard qui leur permettra d'avoir une meilleure interopérabilité avec la plupart des logiciels de gestion vidéo et d'ainsi élargir leur marché. Il s'agit aussi d'un enjeu important pour les manufacturiers de caméras analogiques, tels que Pelco, GE et Honeywell, qui tentent de faire leur entrée dans le marché des caméras IP.

Alors que le standard développé par ONVIF cible la connectivité vidéo, la norme PSIA vise une interopérabilité plus large, couvrant plusieurs plateformes de sécurité, incluant la vidéo IP, les DVR, l'analytique, les accès et l'audio. Au niveau du design, PSIA est bâti comme une API, tandis que les spécifications du ONVIF reposent sur les services Web utilisant des protocoles tels que *Extensible Markup Language* et le *Web Services Description Language*.

⁸⁰ <http://www.siaonline.org/content.aspx?id=4580>.

⁸¹ Honovich, J., *Will ONVIF or PSIA win the IP Camera Standards Battle?*, IP Video Market Info, http://ipvideomarket.info/report/onvif_psia_ip_camera_standards.

L'avenir révèlera qui remportera cette guerre de standards. Peut-être y aura-t-il unification? Le soutien de la Security Industry Association (SIA) pourrait être déterminant pour l'adoption de l'un ou l'autre des standards. C'est pourquoi ONVIF et PSIA travaillent à harmoniser leurs normes avec celles présentement développées par la SIA.

BIBLIOGRAPHIE

LIVRES

- [1] Nilsson, F. "Intelligent Network Video: Understanding Modern Video Surveillance System". Boca Raton: CRC Press, 2009. 389 p.
- [2] Transports Canada. *Réseau de télévision en circuit fermé : manuel de référence pour l'utilisation dans des applications de sécurité*. 2008. 79 p.

ACTES DE CONFÉRENCES, COLLOQUES, ATELIERS

- [3] Cucchiara, R. "Multimedia surveillance systems" dans Proceedings of the third ACM International Workshop on Video Surveillance & Sensor Networks, International Multimedia Conference, pp. 3-10, Singapour, 2005.
- [4] Gagnon, L., Laliberté, L., Foucher, S., Laurendeau, D., Branzan Albu, A. "A System for Tracking and Recognising Pedestrian Faces using a Network of Loosely Coupled Cameras". SPIE Defense & Security: Visual Information Processing XV (SPIE #6246), Orlando, 2006.
- [5] Hampapur, A., Brown, L., Connell, J., Pankanti, S., Senior, A., Tian, Y. "Smart Surveillance: Applications, Technologies and Implications" dans *2003 Joint Conference of the Fourth International Conference on Information, Communications & Signal Processing and Fourth Pacific-Rim Conference on Multimedia*, pp. 1133-1138, vol.2. New York, États-Unis, December 15-18, 2003.
- [6] Sedky, M.H., Moniri, M., Chibelushi, C.C. "Classification of Smart Video Surveillance systems for Commercial Applications". IEEE Conference on Advanced Video and Signal Based Surveillance, Septembre 15-16, 2005. pp. 638-648.
- [7] Xiao, Z., Poursoltanmohammadi, A., Sorell, M. "Video motion detection beyond reasonable doubt", dans *Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*, article no 6, Adelaide, Australie, January 21-23, 2008.

PÉRIODIQUES, MAGAZINES

- [8] Dee, H. M., Velastin, S. A. "How close are we to solving the problem of automated visual surveillance? A review of real-world surveillance, scientific progress and evaluative mechanisms". *Machine Vision and Applications*, 19 (5-6). Septembre 2008. pp. 329-343.

- [9] Foresti, G. L., Micheloni, C., Snidaro, L. Remagnino, P., Ellis, T. « Active Video-Based Surveillance System: The low-level image and video processing techniques needed for implementation ». IEEE Signal Processing Magazine, 22 (2) March 2005. pp. 25-37.
- [10] Hampapur, A., Brown, L., Connel, J., Ekin, A., Haas, N., Lu, M., Merkl H., Pankanti, S., ASenior, A., Shu, C.-F., Tian, Y. L., « Smart Video Surveillance : Exploring the concept of multiscale spatiotemporal tracking », IEEE Signal Processing Magazine, 22 (2) March 2005. pp. 38-51.
- [11] Hearing, N., Venetianer, P. L., Lipton, A. « The evolution of video surveillance: an overview». Machine Vision and Applications, 19 (5-6) September 2008 : pp. 279-290.
- [12] Hu, W., Tieniu, T., Wang, L., Maybank, S. « A Survey on Visual Surveillance of Object Motion and Behaviors ». IEEE Transactions on systems, man, and cybernetics-Part C: Applications and reviews, 34(3), août 2004, pp. 334-352.
- [13] Kosk, N., « OnSSI Secures 2008 Political Conventions ». Video Technology & Applications, Février 2009 : pp. 6-10.
- [14] Zhan, B., Monekosso, D. N., Remagnino, P., Velastin, S. A., Xu, L.-Q. "Crowd analysis: a survey", Machine Vision and Applications, 19 (5-6) Septembre 2008. pp. 345-357.

RAPPORTS TECHNIQUES

- [15] Axis Communications, *H.264 video compression standard. New possibilities within video surveillance*. Document technique. 2008. 9 p.
- [16] Biale, N. *Expert Findings on Surveillance Cameras: What Criminologists and Others Studying Cameras Have Found*. American Civil Liberties Union. 29 mai 2008, 6 p.
- [17] Fullerton, E. *Enabling Video Analytics - The advantages of an open platform IP video surveillance management solution for enaling video analytics*. White Paper, Milestone Systems, 2008, 20 p.
- [18] Gager, R. Special Report: Video Surveillance, State of the Market, SDM, vol. 38, no 3, p. 68.
- [19] Hewitson, N. *Video Content Analysis, shat is it and why would I want it*. White Paper, Smart CCTV Limited, 2005. 3 p.
- [20] Honovich, J., *Security Manager's Guide to Video Surveillance*. Version 2.0, IPVideoMarket.info, Novembre 2008, 131 p.

- [21] Institute of Management and Administration, Inc. *Security's Director Report*, Newsbrief, Février 2009.
- [22] King, et al. *CITRIS Report: The San Francisco Community Safety Camera Program – An Evaluation of the Effectiveness of San Francisco's Community Safety Cameras*. Décembre 2008, 184 p.
- [23] Kirstein, M. *The expanding World of IP Video Surveillance: Cameras, Storage, Technology and Semiconductors*. Multimedia Intelligence, 2008. 10 p. [MMI080405WP].
- [24] McNichol, J. Lav, I. J., *State Budget Troubles Worsen*, Center on Budget and Policy Priorities, 13 mars 2009.
- [25] Senior, A., Pankanti, S., Hampapur, A., Brown, L. Tian, Y.-L., Ekin, A. *Blinkering Surveillance: Enabling Video Privacy through Computer Vision*. IBM Research Report. 28 août 2003, 14 p. [RC22886 (W0308-109)].

PRÉSENTATIONS

- [26] Diamant, M. *Why is Everyone Migrating to Intelligent IP Video Surveillance?* ISC East, 29 octobre 2008.
- [27] Gorodnichy, D. *Systèmes de reconnaissance vidéo, Vidéotechnologie pour la sécurité : problèmes et solutions*. Atelier sur la sécurité du transport ferroviaire et urbain, Montréal, Novembre 2007.
- [28] Moellman, D. *VACE Program Manager Video Analysis and Content Extraction (VACE) R&D Program: Overview of Phase 2*. Novembre 2003.

RÉFÉRENCES ÉLECTRONIQUES COMPLÉMENTAIRES À CELLES CITÉES DANS LE TEXTE

(Note : Toutes les références électroniques étaient en ligne le 28 mars 2009)

Sécurité et vidéosurveillance

Castonguay, A. *La loi, l'ordre et la sécurité restent des priorités conservatrices*, Le Devoir, 27 février 2008, <http://www.ledevoir.com/2008/02/27/177974.html>.

Ministère des Relations internationales du Québec, *Contribuer à la sécurité du Québec et du continent nord-américain*,
http://www.mri.gouv.qc.ca/fr/politique_internationale/securite/index.asp.

Siemon, *CCTV & Video Surveillance over 10G ip™*,
http://www.siemon.com/us/white_papers/03-10-29-cctv.asp.

Wasatis, *Historique*, <http://www.wasatis.com/spip/spip.php?article5>.

Kammerer, D. *Police use of public video surveillance in Germany 1956: management of trafic, repression of flows, persuasion of offenders*, *Surveillance & Society*, Vol. 6, No 1 (2009), http://www.siemon.com/us/white_papers/03-10-29-cctv.asp.

Fullerton, E., *The History of Video Surveillance*, Milestone,
http://www.milestonesys.com/files/UserFiles/Articles/History_of_Video_Surveillance.pdf.

Wikipedia. *Vidéosurveillance*. <http://fr.wikipedia.org/wiki/Vidéosurveillance>.

Wikipedia. *Video Analytics*. http://en.wikipedia.org/wiki/Video_analytics.

Office québécois de la langues française, *Grand dictionnaire terminologique*,
<http://www.granddictionnaire.com>.

VideoAnalytics.net, *What Is Video Analytics / Intelligent Video Surveillance*,
<http://www.videoanalytics.net/articles/whatisva.html>.

Vlahos, J. *Surveillance Society: New High-Tech Cameras Are Watching You*,
PopularMechanics, janvier 2008,
http://popularmechanics.smartmoney.com/technology/military_law/4236865.html?page=1.

Cager, Y. *Smart Video Surveillance: Digital Technology vs. Tradition Analog Systems*,
Advanced Imaging Magazine, 8 juillet 2008,
<http://www.advancedimagingpro.com/publication/article.jsp?pubId=1&id=2537&pageNum=1>.

Vision Industrielle.Org, *Qu'est-ce que la télésurveillance intelligente ?*,
<http://www.visionindustrielle.org/visionwhat-remotemonitoring.php>.

VisioWave, *Intelligent Security Applications, Image Processing And Video Content Analysis*, <http://www.visiowave.com/index.asp?index=intelligentVideo>.

Freschi, C., *A Smart Future for Video Surveillance*, *Security Magazine*, 1^{er} janvier 2009,
http://www.securitymagazine.com/Articles/Column/BNP_GUID_9-5-2006_A_10000000000000364844.

IP Video Market Info, *Video Analytics Overview and News*,
<http://ipvideomarket.info/topics/VideoAnalytics>.

Honovich, J., *Top 3 Problems Limiting the Use and Growth of Video Analytics*, IP Video Market Info, 19 juin 2008, http://ipvideomarket.info/report/top_3_problems_limiting_the_use_and_growth_of_video_analytics

Automated Video Systems, *Video Surveillance made simple*, <http://www.ezwatch-security-cameras.com/downloads/>

Thomas, S. *Out-of-the-box Thinking—The Transition Away from Analog CCTV and DVRs to IP Video*, LossPreventionMagazine.com, 14 octobre 2008, http://www.losspreventionmagazine.com/wparchives_view.html?id=2234.

Hu, Y. H., *Survey of Video Surveillance Technology*, www.ece.wisc.edu/~facerec/cameranet/survey2008Oct03.ppt.

Honovich, J., *Should I Use IP Cameras? Re-Assessing IP Camera's Advantages*, IP Video Market Info, 14 mai 2008, http://ipvideomarket.info/report/should_i_use_ip_cameras_reviewing_ip_camera_advantages.

Honovich, J., *Top 5 IP Camera Problems*, 26 juillet 2008, IP Video Market Info, http://ipvideomarket.info/report/top_5_ip_camera_problems.

Digital Visions Security Technologies, *Digital IP Video Surveillance*, http://www.digitalvisionsllc.com/digital_ip_video_surveillance_systems.aspx.

VideoSurveillance.com, <http://www.videosurveillance.com>.

Applications

Genetec, *Solutions innovatrices*, <http://www.genetec.com/Francais/Solutions/Pages/solutions.aspx>.

VideoSurveillance.com, www.videosurveillance.com.

IndigoVision, *Whatever your business*, <http://www.indigovision.com/business.php#it>.

Osborn, A., *Top 7 non-security uses for video surveillance cameras -- more than just a crime prevention tool*, Video-Surveillance-Guide.com, <http://www.video-surveillance-guide.com/video-surveillance-cameras.htm>.

Industry Solutions, VideoSurveillance.com, <http://www.videosurveillance.com/industry-solutions/>.

Salvi, D. V., *A Clear View: Megapixel cameras playing into the gaming surveillance market*, 3 mars 2009, <http://www.secprodonline.com/Articles/2009/03/03/A-Clear-View.aspx>.

Bombardier, *Intégration d'un système de sécurité dans les trains de passagers*, 7 décembre 2006, http://www.aqtr.qc.ca/documents/14_AllocutionsConferences/7_decembre_ReneMeuser.pdf.

Transports Québec, Gestion de la circulation,
http://www.mtq.gouv.qc.ca/portal/page/portal/regions/montreal_ile/gestion_circulation.

Composantes et architecture d'un système de surveillance

BSI Alès, *Les différents types de caméras sur réseau informatique*,
<http://www.bsi.fr/Informatique/Informatiquedentreprise/Vid%C3%A9osurveillance/tabid/73/articleType/ArticleView/articleId/6/Default.aspx>.

Honovich, J., *Examining the Future of Video Surveillance Storage*, IP Video Market Info, 6 août 2008,
http://ipvideomarket.info/report/examining_the_future_of_video_surveillance_storage.

Honovich, J., *Should You Use Video Encoders?*, IP Video Market Info, 18 mars 2009,
http://ipvideomarket.info/report/video_surveillance_analog_encoders.

Grossman, R. *The Nuances of Network Video Recorder, Security Sales & Integration*, Août 2006, http://www.securitysales.com/t_inside.aspx?action=article&StoryID=2529.

Honovich, J., *Analytics - To Lead or Not to Lead*, IP Video Market Info, 19 septembre 2008, http://ipvideomarket.info/report/analytics_to_lead_or_not_to_lead.

Mobotix AG, http://www.mobotix.com/fre_CH/content/view/full/2.

Honovich, J., *Upcoming Panoramic Megapixel Camera from Scallop*, IP Video Market Info,
http://ipvideomarket.info/report/upcoming_panoramic_megapixel_camera_from_scallop.

Recherche, entreprises, produits commerciaux et fonctionnalités intelligentes

Carnegie Mellon University, Robotics Institute, *Overview*, <http://www.cs.cmu.edu/~vsam/>.

Networks & Organizations, *The Intelligence Community Invests in Video*, 9 mars 2006,
<http://www.intelligenceonline.com/c/illustrations/io/pdf/INT518%208.pdf>.

IBM, *IBM Smart Surveillance System (S3)*, <http://www.research.ibm.com/peoplevision/>.

Organix IT, <http://www.organixit.com>.

YouTube, *Trends and Solutions for Video Surveillance Market*,
<http://www.youtube.com/watch?v=l031ca0j7gk>.

Home Security Blog, *Video surveillance enhancements for Airport security*, 20 août 2008, <http://www.2mcctv.net/blog/content/view/69/26/>.

Honovich, J., *Upcoming Panoramic Megapixel Camera from Scallop*, IP Video Market Info, 9 janvier 2009, http://ipvideomarket.info/report/upcoming_panoramic_megapixel_camera_from_scallop.

Industrie Canada, *Répertoire d'entreprises par secteur industriel*, <http://www.ic.gc.ca/eic/site/company-entreprises.nsf/fra/accueil>.

Industrial Embedded Systems, *Matrox Graphics Unveils IP Video Decoding Accelerator for Surveillance Systems*, 17 novembre 2008, <http://www.industrial-embedded.com/news/db/?14296>.

Honovich, J., *Wireless Video Surveillance Tutorial*, IP Video Market Info, http://ipvideomarket.info/report/wireless_video_surveillance_tutorial.

ExpertsDuRisque.com, *Les softs d'analyse d'image*, http://www.expertsdurisque.com/annuaire/site/FR/Dossiers_produits/Dossiers_Securite/Les_softs_danalyse_dimage,I2404.htm?xtor=SEC-15.

ISC-West 2009, *Exhibitor list*, http://iscwest09.mapyourshow.com/2_1/search.cfm?let=@.

Reconnaissance faciale

Osborn, A., *How biometric technology is used in video surveillance*, <http://www.video-surveillance-guide.com/biometric-technology.htm>.

Face Recognition Homepage, <http://www.face-rec.org/general-info/>.

Woodward, J. D. et al., *Biometrics: A look at Facial Recognition*, http://electronics.howstuffworks.com/framed.htm?parent=facial-recognition.htm&url=http://www.rand.org/pubs/documented_briefings/DB396/DB396.pdf.

Howstuffworks, *Face Recognition*, <http://electronics.howstuffworks.com/framed.htm?parent=facial-recognition.htm&url=http://www.epic.org/privacy/facerecognition>.

Airport International, *3D face recognition technology*, <http://www.airport-int.com/categories/3d-face-recognition-technology/3d-face-recognition-technology.asp>.

Face Recognition Vendor Test 2006, <http://www.frvt.org/FRVT2006/default.aspx>.

Bryner, J., *Computers Get Better at Face Recognition*, Live Science, 24 janvier 2008, <http://www.livescience.com/technology/080124-face-recognition.html>.

Enjeux

Les chroniques judiciaires de Me Alain P. Lecours, *Vidéo surveillance en milieu de travail & protection de la vie privée*, <http://www.lecourslessard.com/droit-travail-video-surveillance-en-milieu-de-travail-protection-de-la-vie-privee.html>.

Conger, C., *Do police cameras reduce crime?*, Howstuffworks, <http://electronics.howstuffworks.com/police-camera-crime.htm>.

University of Victoria, *Does Video Surveillance Prevent Crime?*, <http://socialsciences.uvic.ca/about/VideoSurveillanceandCrime.htm>.

ANNEXE 1 - Programmes de recherche majeurs en vidéosurveillance intelligente

Cette annexe donne une liste de certains programmes de recherche qui ont fortement contribué au développement de technologies analytiques pour la vidéosurveillance. Ces programmes et projets ont permis de financer des travaux de recherche dans les universités et les entreprises, qui ont souvent débouchés sur la commercialisation de technologies d'analyse vidéo pour la sécurité.

Projet	Description
Annotated Digital Video for Surveillance and Optimised Retrieval (ADVISOR) (Communauté européenne), 2000-2003 http://www.ist-world.org/ProjectDetails.aspx?ProjectId=3c4d4b1710844de5962bc5f91f7ec5c8	L'objectif de ce projet était de développer des outils logiciels pour la vidéosurveillance intelligente dans les transports publics. Il visait le développement de techniques pour la détection de mouvement, le suivi de personnes, la reconnaissance de comportements, la surveillance d'individus et de foules.
BEHAVE (Royaume-Uni., EPSRC), 2007 http://www.secure-force.eu/index.php?option=com_content&task=view&id=155&Itemid=9	L'objectif de ce projet est de développer des technologies pour détecter les comportements suspects dans les lieux publics, à partir de la vidéo provenant d'un réseau de plusieurs caméras.
Combat Zone That See (DARPA, États-Unis), 2003 http://www.atec-tec.net/fr/its_news_det.asp?code_news=1404	Programme qui fut lancé par l'armée américaine, sous la direction de la DARPA (Defense Advanced Research Projects Agency) et qui visait la surveillance dans les zones de conflits urbains grâce à un réseau de caméras. L'objectif était de développer des logiciels permettant de traiter l'information provenant des différentes caméras pour identifier les véhicules (type, couleur, et plaque d'immatriculation), les conducteurs et les événements suspects.
Context Aware Vision using Image-based Active Recognition (CAVIAR) (Communauté européenne), 2002-2005 http://homepages.inf.ed.ac.uk/rbf/CAVIAR/caviar.htm	Financé par la Information Society Technology, ce programme visait, entre autres, la reconnaissance d'objets, de contexte et de situations pour la surveillance urbaine et les analyses marketing.
Integrated Surveillance of Crowded Areas for Public Security (ISCAPS) (Europe) (consortium de dix entreprises et institutions académiques), 2005 http://www.iscaps.reading.ac.uk/	Mené par un consortium de dix entreprises et institutions académiques, ce projet vise la surveillance de foules et des lieux achalandés. Il vise notamment le développement d'outils biométriques pour l'identification de personnes.

Projet	Description
Pro-active Integrated Systems for Security Management by Technological Institutional and Communications (PRISMATICA) (Communauté européenne), terminé en 2002 http://tf1.lci.fr/infos/high-tech/2001/0,,818766,00-prismatica-informatique-service-securite-transports-.html	Initié par six transporteurs européens, ce projet vise à renforcer la sécurité dans les transports publics, en développant des outils logiciels pour l'analyse des images de surveillance. Elle touche notamment à la détection de personnes et d'objets, ainsi qu'à l'analyse de leurs comportements, pour détecter des colis suspects ou des vols, par exemple.
Video Analysis and Content Extraction (VACE) (DTO, Etats-Unis) – Phase 3 : 2006-2009 http://www.perceptual-vision.com/vt4ns/vace_brochure.pdf	Programme mené par le Disruptive Technology Office (DTO), relevant du Director of National Intelligence (DNI). Il a pour objectif de développer des technologies d'analyse et d'indexation de la vidéo provenant de différentes sources, en particulier celle captée par les caméras de surveillance. Les recherches dans ce programme portent, notamment, sur l'extraction de données significatives à partir de la vidéo, la fusion multimodale, la reconnaissance et la compréhension de comportements.
Video Surveillance and Monitoring (VSAM), 1997-2000 http://www.cs.cmu.edu/~vsam/OldVsamWeb/vsamhome.html	Lancé et financé par le Information Systems Office de la Defense Advanced Research Projects Agency (DARPA), aux États-Unis. Il s'agit de l'un des premiers projets d'analyse en temps réel de données de vidéo surveillance pour l'intervention et la prévention d'incidents. L'objectif de ce projet était de développer la vidéo automatisée et la rendre capable de comprendre et évaluer l'information reçue pour l'utilisation dans des applications militaires de surveillance des zones urbaines ou de combat. La recherche portait, entre autres, sur la surveillance de zones étendues, la détection et le suivi d'objets en temps réel, la reconnaissance d'objets, le comptage de véhicules, le contrôle actif de caméras, la reconnaissance d'activités humaines.

ANNEXE 2 - Groupes de recherche (Québec et États-Unis)

Cette annexe présente une liste de groupes de recherche au Québec, qui œuvrent en analyse vidéo pour la vidéosurveillance intelligente. Les laboratoires universitaires américains ayant une contribution majeure dans ce domaine y sont aussi répertoriés. La plupart d'entre eux ont, notamment, participé au programme de recherche VACE.

Laboratoire/Groupe	Description des travaux
Québec	
Laboratoire de Vision et Systèmes Numériques, Université Laval http://vision.gel.ulaval.ca/	Reconnaissance d'activités humaines. Modélisation de la démarche humaine. Détection et suivi d'objet. Réseau de caméras intelligentes. Participation au projet MONNET sur la surveillance d'environnements complexes et le suivi de personnes à l'aide d'un réseau faiblement couplé de caméras (http://vision.gel.ulaval.ca/fr/Projects/IdEns_41/index.php)
LITIV, École Polytechnique de Montréal http://www.polymtl.ca/litiv/en/	Traitement d'images et de la vidéo, entre autres, pour des applications de vidéosurveillance.
LIVIA, École de technologie supérieure http://www.livia.etsmtl.ca/membres.php?LANG=en	Reconnaissance de visages en environnements non contraints.
VidPro, Université Concordia http://users.encs.concordia.ca/~vidprog/	Détection et suivi d'objets, même sous occlusions. Détection d'événements. Application à la vidéosurveillance.
Groupe Vision et imagerie, CRIM http://www.crim.ca/fr/r-d/vision_imagerie/index.html	Détection et suivi d'objets, détection et reconnaissance de visages, reconnaissance d'expressions faciales, reconnaissance de plaques d'immatriculation, reconnaissance de mouvements anormaux, indexation de banques vidéo. Le groupe a mené plusieurs projets en vidéosurveillance pour la sécurité, dont MONNET, PTZ et VISU (http://www.crim.ca/fr/r-d/vision_imagerie/projets.html).
Visual Motor Research Lab, Université McGill http://www.cim.mcgill.ca/~clark/vmrl/web-content/vmrl.html	Détection d'anomalies pour la vidéosurveillance.
États-Unis	
Computer Vision Laboratory, University of Maryland http://www.cfar.umd.edu/cvl/	Reconnaissance d'objets. Détection et suivi de véhicules et d'humains. Caractérisation de la démarche humaine et reconnaissance faciale. Détection de la taille d'un individu. Indentification de personnes dans les foules. Détection d'objets abandonnés.

Laboratoire/Groupe	Description des travaux
Computer Vision Lab, University of Central Florida http://server.cs.ucf.edu/~vision/	Détection et suivi d'objet, reconnaissance d'activités humaines, analyse de foules et suivi d'individu dans des environnements peuplés.
Face Recognition and Video Processing Lab, New Jersey Institute of Technology http://www.cs.njit.edu/liu/FRVPlab/index.html	Reconnaissance de visages.
Informedia, Carnegie Mellon University http://www.informedia.cs.cmu.edu/	Participe au programme de recherche VACE. Indexation et recherche de contenus vidéo. Détection des personnes et patrons d'activité dans des images vidéo. Méthodes de protection des informations privées sur la vidéo visionnées par plusieurs usagers.
Institute for Robotics and Intelligent Systems, University of Southern California http://iris.usc.edu/	Participe au programme VACE. Détection et suivi d'objets et d'humains pour la vidéosurveillance. Reconnaissance d'activités et d'événements.
Robotics Institute, Carnegie Mellon University http://www.ri.cmu.edu/	Différents groupes couvrent des aspects de recherche applicables à la vidéosurveillance : détection et suivi de personnes, détection et reconnaissance faciale, identification de personnes, reconnaissance de gestes et de comportements humains.
Vision Research Group, Massachusetts Institute of Technology http://groups.csail.mit.edu/vision/app/	Avait participé au programme de recherche VISAM. Techniques d'analyse vidéo dans un réseau distribué de caméras : détection, suivi et reconnaissance d'objets, classification d'activités, détection d'événements normaux et anormaux.

Annexe 3 - Entreprises en vidéosurveillance (Québec et autres)

Étant donné le nombre considérable d'entreprises offrant des produits et des services en vidéosurveillance, il aurait été impossible d'en donner une liste exhaustive. Cette annexe présente les principales entreprises qui ont été trouvées suite à des recherches sur le Web, à la consultation des experts et aux rencontres faites lors des conférences ISC-West 2008 et ISC-East 2008. Des recherches particulières ont été menées pour répertorier les entreprises québécoises, ainsi que celles provenant des autres provinces canadiennes, développant des produits en vidéosurveillance numérique intelligente. Celles-ci sont énumérées en premier dans chaque catégorie de services. Cependant, les intégrateurs, installateurs et distributeurs en vidéosurveillance n'ont pas tous été recensés.

Des listes plus complètes d'entreprises dans le domaine de la sécurité et de la vidéosurveillance peuvent être trouvées, notamment sur :

- http://www.canasa.org/en/membership/mem_directory/index.html.
- <http://www.sourcesecurity.com/companies.html>.
- <http://www.videosurveillance.com/manufacturers/>.
- <http://ipvideomarket.info/>.
- <http://www.iscwest.com/App/homepage.cfm?appname=180&moduleID=2958&LinkID=20077&submenuheader=7>.

Les descriptions des entreprises ont été tirées ou adaptées des références Web ci-dessus ou du site Internet des entreprises.

Grands manufacturiers et fournisseurs offrant des produits de sécurité et vidéosurveillance	
Axis Communications (Suède) www.axis.com	Axis est le leader mondial du marché de la vidéo sur IP. Société suédoise fondée en 1984, elle dispose de filiales dans plus de 20 pays et travaille en coopération avec de nombreux partenaires dans plus de 70 pays. Axis s'est spécialisée dans les solutions professionnelles de vidéo sur IP destinées à la surveillance, la télésurveillance et la diffusion. Cette gamme de produits comprend des caméras réseau, des serveurs vidéo, des décodeurs vidéo, des logiciels de gestion vidéo, ainsi qu'un ensemble complet d'accessoires.
Bosch Security Systems (Allemagne) www.boschsecurity.com	Bosch Security Systems offre différents produits de sécurité, dont des systèmes de vidéosurveillance, incluant des solutions IP.
Checkpoint Systems (États-Unis) www.checkpointsystems.com	Checkpoint Systems offre une gamme complète de produits et services en sécurité, notamment des systèmes de vidéosurveillance.
Cisco (États-Unis) www.cisco.com	Cisco offre une solution complète de vidéosurveillance qui s'intègre à ses équipements de réseau. L'entreprise vend notamment des encodeurs (fournis par SyPixx) et un logiciel de gestion vidéo (développé par Broadware) qui peut fonctionner sur les routeurs de Cisco. Ce géant des TI commercialise aussi deux caméras IP.
D-Link (Taiwan) www.dlink.com/products/end-to-end-surveillance	À travers ses partenariats avec les manufacturiers et développeurs de composantes de vidéosurveillance, D-Link offre des solutions complètes de vidéosurveillance IP.
GE Security (États-Unis) www.gesecurity.com	GE Security vend différents systèmes de sécurité, dont des outils de vidéosurveillance. L'entreprise offre même un logiciel de gestion vidéo intelligent (VisioWave Intelligent Video Platform).
Honeywell Security (États-Unis) www.honeywellvideo.com	Honeywell Security est un fournisseur et un distributeur international de systèmes électroniques de sécurité. L'entreprise commercialise Digital Video Manager, une solution de vidéosurveillance numérique en réseau basée sur une architecture ouverte.
JVC (États-Unis) www.pro.jvc.com	Géant de l'électronique, JVC vend des caméras analogiques, mais manufacture aussi une gamme de caméras et d'accessoires de surveillance IP. L'entreprise produit aussi des enregistreurs numériques réseau (NVR).
Mitsubishi (Japon) www.mitsubishi.com	À travers ses différentes divisions, Mitsubishi manufacture plusieurs produits de vidéosurveillance, dont des enregistreurs numériques, des murs d'écrans et, plus récemment, des caméras IP.
Panasonic (Japon) www.panasonic.com/business/security/home.asp	Panasonic est l'un des principaux manufacturiers de caméras analogiques. L'entreprise développe aussi une gamme d'enregistreurs numériques et de caméras IP pour la surveillance. Celles-ci viennent sous différentes formes : mégapixel, PTZ, dôme.

Grands manufacturiers et fournisseurs offrant des produits de sécurité et vidéosurveillance	
Pelco (États-Unis) www.pelco.com	Pelco est l'une des plus grandes entreprises en vidéosurveillance et le leader des manufacturiers de caméras analogiques. L'entreprise offre une gamme étendue de composantes de vidéosurveillance, dont des solutions de gestions vidéo sur enregistreur numérique, traditionnel ou hybride, et sur enregistreur réseau. Pelco s'est lancée dans le marché des caméras IP en commercialisant quelques modèles.
Samsung GVI (États-Unis) www.gviss.com	Samsung GVI offre une suite complète de solutions de vidéosurveillance et de solution intégrées de sécurité qui permettent la vidéosurveillance intelligente.
Toshiba (Japon) www.toshiba.com	Toshiba offre une gamme complète de produits de vidéosurveillance, incluant des caméras analogiques et IP, moniteurs, enregistreurs numériques et réseau. Ses caméras IP sont réputées pour la qualité de leur image dans des conditions de faible illumination.
Tyco International (Bermudes) www.tyco.com	Tyco International est une entreprise diversifiée offrant des produits et des services dans 60 pays. Elle commercialise une gamme étendue de technologies de contrôle d'accès et de vidéo sous ses différentes marques : Software House, American Dynamics and Kantech.
Vicon (États-Unis) www.vicon-cctv.com	Vicon développe, manufacture et commercialise des solutions complètes sur réseau IP pour intégrer la vidéosurveillance avec le contrôle d'accès. L'entreprise offre des logiciels de gestion vidéo, des enregistreurs numériques et réseau, des encodeurs et décodeurs, ainsi que des caméras (IP, mégapixel, analogiques, dôme).

Logiciels de gestion vidéo et système de vidéosurveillance IP	
Genetec (Québec) www.genetec.com	Genetec est l'un des plus grands développeurs de logiciel de vidéosurveillance IP. Il développe Omnicast™, une solution de vidéosurveillance sur IP. Ce logiciel intègre les technologies d'analyse vidéo de partenaires. Celles-ci permettent la détection et l'identification d'objets et d'individus, ainsi que la reconnaissance de comportements inhabituels. La solution AutoVu permet la reconnaissance automatisée de plaques d'immatriculation dans des applications fixes et mobiles.
Aimetis (Ontario) www.aimetis.com	Aimetis développe un logiciel de gestion vidéo, supportant les caméras analogiques et numériques, qui intègre des bibliothèques de fonctions d'analytique vidéo pour des applications spécifiques. L'entreprise développe notamment des algorithmes propriétaires de détection et de suivi d'objets (voitures/personnes) fonctionnant sous des conditions changeantes d'illumination et de météo, de comptage de personnes, de détection et classification d'événements tels que les intrusions, les stationnements interdits et les fraudes au guichet automatique. Ses marchés principaux touchent aux applications de surveillance extérieure et au commerce de détail.
Impath Networks (Nouvelle-Écosse) www.impathnetworks.com	Impath offre i-Volution, une gamme de produits de vidéosurveillance sur réseau IP, ainsi que TeleVue, un logiciel de gestion d'application permettant de configurer et contrôler l'équipement vidéo en réseau.
March Networks (Ontario) www.marchnetworks.com	March Networks commercialise la gamme de produits VideoSphere pour la vidéosurveillance IP sur des réseaux filaires ou sans fil. L'entreprise offre des caméras IP, des enregistreurs numériques, des encodeurs et un logiciel de gestion vidéo. Ce dernier inclut des fonctionnalités d'analytique pour la surveillance aux points de vente. Son principal compétiteur est Verint.
AMAG Technology (Royaume-Uni) www.amag.com	AMAG Technology développe un système de gestion de la sécurité pour l'industrie et les gouvernements. Celui-ci comprend <i>Symmetry Video</i> , une plateforme ouverte de gestion vidéo pour les serveurs vidéo, les enregistreurs vidéo numériques et les caméras IP.
American Dynamics (États-Unis, une entreprise de Tyco) www.americandynamics.net	La famille de produits Intellex® offre des solutions de surveillance vidéo intégrant systèmes analogiques et IP. L'entreprise est l'un des plus gros vendeurs d'enregistreurs numériques au monde. Elle a acquis, en 2008, Intellivid, compagnie spécialisée en analytique vidéo.
Aventura Technologies (États-Unis) www.aventuratechnologies.com	Aventura Technologies développe un logiciel de gestion vidéo qui possède les fonctionnalités standards de navigation dans la vidéo. Il inclut aussi des fonctions d'analytiques vidéo, telles que la détection de personnes basée sur la couleur et la texture de la peau, la détection et le suivi d'objets et la reconnaissance d'activités. Ces détections nécessitent un paramétrage chez le client.
Exacq (États-Unis) www.exacq.com	Exacq Technologies Inc. développe un système de gestion vidéo à architecture ouverte dont la qualité est reconnue.

Logiciels de gestion vidéo et système de vidéosurveillance IP	
IBM (États-Unis) www.ibm.com	IBM offre des solutions intégrées de vidéosurveillance et de sécurité. L'entreprise mène aussi des travaux de recherche dans le domaine de l'analytique vidéo. Elle commercialise un système de vidéosurveillance intelligente basé sur une architecture ouverte.
IndigoVision (Royaume-Uni) www.indigovision.com	IndigoVision offre une solution de vidéosurveillance IP de bout en bout. Sa ligne de produit comprend des caméras IP, des encodeurs, des enregistreurs sur réseau et un logiciel de gestion vidéo. L'entreprise développe son propre CODEC. Ses produits ne supportent pas les caméras de concurrents. En 2008, IndigoVision a obtenu un contrat de plusieurs millions de dollars de l'Agence des services frontaliers du Canada, pour déployer des caméras IP aux postes frontaliers entre le Canada et les États-Unis
Milestone (Danemark) www.milestonesys.com	Milestone développe la plateforme de gestion de vidéosurveillance IP ouverte Milestone XProtect™. L'interface permet d'intégrer plusieurs modules d'analytique vidéo. Cette entreprise se spécialise dans le logiciel et ne vend pas de composantes matérielles. Son logiciel supporte un grand nombre de caméras et systèmes de sécurité sur le marché.
Mosaic Dynamic Solutions (États-Unis) www.mosaicdyns.com	Mosaic Dynamic Solutions offre plusieurs produits pour la surveillance et le suivi des actifs d'une organisation. L'entreprise commercialise des solutions d'analytique vidéo permettant la détection d'objets, la reconnaissance de comportements suspects, la reconnaissance de visages et de plaques d'immatriculation.
Nice Systems (Israël) www.nice.com	Nice fournit des solutions complètes de sécurité, notamment des produits de vidéosurveillance. Nice Inform capture et synchronise des données multimédia pour la surveillance (voix, vidéo, texte, etc.) pour les fins d'enquêtes.
OnSSI, On-Net Surveillance Systems Inc. (États-Unis) www.onssi.com	OnSSI développe Ocularis, un logiciel de gestion vidéo IP qui comprend une interface sophistiquée offrant plusieurs outils de navigation et de visualisation à l'utilisateur.
Video Insight (États-Unis) www.video-insight.com	Video Insight développe une suite étendue de modules logiciels pour la gestion de la vidéosurveillance.
3VR (États-Unis) www.3vr.com	3VR commercialise un logiciel de gestion vidéo pour la surveillance permettant des recherches avancées grâce à des outils intégrés d'analytique vidéo (reconnaissance de visages, reconnaissance de plaques d'immatriculation, détection de mouvement).

Caméras	
ImmerVision (Québec) www.immervision.com	Immervision commercialise la technologie brevetée Panomorphe, qui comprend une lentille grand angle accompagnée d'algorithmes de gestion de la distorsion. Cette lentille offre un champ de vision oval de 360° par 180°, dont la résolution ne diminue pas en périphérie. Elle s'adapte sur une caméra ordinaire, ce qui constitue un net avantage commercial sur son principal concurrent, Grandeye. La lentille Panomorphe utilise 33 % plus de pixels que la technologie <i>fish eye</i> . Toutes les vues PTZ sont recréées numériquement. L'entreprise offre aussi une librairie logicielle gratuite permettant de gérer l'affichage des images vidéo et la navigation dans celles-ci. Cette librairie peut être intégrée aux enregistreurs numériques et réseau.
Avigilon (Colombie-Britannique) www.avigilon.com	Bien qu'elle offre des caméras IP, des encodeurs et des logiciels de gestion vidéo, Avigilon se spécialise dans les caméras mégapixel (jusqu'à 16 mégapixels) et l'optimisation de la vidéosurveillance en haute définition. Ces produits sont particulièrement bien adaptés pour les environnements extérieurs. Cette entreprise supporte peu de systèmes de tiers.
Lumenera (Ontario) www.lumenera.com	Lumenera commercialise une gamme de caméras mégapixel (jusqu'à 11 mégapixels), sensibles à de faibles éclairages. Supporte l'analytique vidéo pour leur série <i>li</i> et est partenaire de ObjectVideo.
ACTi (Taiwan) www.acti.com	ACTi offre une gamme complète de caméras IP de bonne qualité à bas prix, ainsi que des logiciels d'enregistrement sur réseau. Les caméras d'ACTi sont supportées par plusieurs fabricants d'enregistreurs numériques. Les caméras de l'entreprise constituent souvent une alternative moins coûteuse par rapport aux caméras d'Axis.
Arecont Vision (États-Unis) www.arecontvision.com	Arecont Vision offre une ligne complète de caméras mégapixel (jusqu'à 8 mégapixels), à des prix inférieurs à ses principaux concurrents, IQInVision et Lumenera. En 2008, l'entreprise a commencé à supporter la compression H.264, ce qui pourrait avoir un impact majeur sur l'industrie.
Grandeye (Royaume-Uni) http://www.grandeye.com/	GrandEye commercialise des caméras panoramiques, en versions analogiques ou IP. La version IP offre cinq mégapixels de résolution. Ses principaux concurrents sont Mobotix et ImmerVision.
Ipix Corporation (États-Unis) www.ipix.com	IPIX a développé l'un des premiers systèmes permettant de produire des images 360° par 360° (<i>fish eye</i>) dans lesquelles on peut naviguer. En sécurité, Grandeye commercialise la technologie d'IPIX sous une marque conjointe.
IQinVision (États-Unis) www.iqeye.com/	IQinVision commercialise des caméras mégapixels et intelligentes. L'entreprise est implantée dans le marché de la vidéosurveillance en haute définition depuis 1998. Elle offre des caméras jour/nuit, des caméras à dôme résistantes aux vandalisme et des caméras IP résistantes aux intempéries.
Linksys (États-Unis, une entreprise de Cisco) www.linksys.com	Linksys fournit des caméras numériques sans fil se connectant à un réseau. Les solutions offertes par Linksys visent les petites entreprises et les résidences.

Caméras	
Logitech (États-Unis) www.logitech.com	Logitech manufacture des webcams de surveillance pour le grand public.
Mobotix (Allemagne) www.mobotix.com	Mobotix commercialise des caméras réseau haute résolution et des systèmes de vidéosurveillance décentralisés. L'entreprise occupe la deuxième place du secteur en Europe et la quatrième au niveau mondial. Avec une résolution de 3,1 mégapixels, les caméras MOBOTIX offrent une image 30 fois plus précise que les caméras analogiques. C'est pourquoi elles permettent de surveiller des zones plus vastes, avec une vision à 360°, réduisant ainsi le nombre de caméras requises et les coûts s'y rattachant.
Scallop Imaging (États-Unis) www.scallopimaging.com	Cette entreprise produit la caméra D7, une caméra de sept mégapixels pour la surveillance, fournissant un champ de vision de 180° sans aucune distorsion de l'image.
Theia (États-Unis) http://www.theiatech.com/	Theia produit des lentilles grand angle pour les caméras mégapixels, permettant de couvrir une très large zone de surveillance.
Vivotek (Taiwan) www.vivotek.com	Vivotek offre une vaste gamme de caméras IP économiques. Il est le plus grand fournisseur dans le segment de marché bas de gamme pour les consommateurs et les petites entreprises.

Sans fil	
Réseaux Eagle (Québec) www.reseauxeagle.com	Cette entreprise se spécialise dans le déploiement, la gestion et la sécurité de réseaux sans fil, notamment pour la vidéosurveillance. Elle est spécialiste des réseaux de type 802.11.
Firetide (États-Unis) www.firetide.com	Firetide fournit des produits pour l'infrastructure et l'accès dans les réseaux maillés à transmission sans fil. Elle offre des solutions spécialisées pour la vidéosurveillance, mais aussi pour la téléphonie et les données. Les produits de Firetide ont été implantés à Phoenix pour la surveillance du Super Bowl 2008.
Strix Systems (États-Unis) www.strixsystems.com	Strix Systems est un fournisseur d'équipements pour les réseaux sans-fil maillés. Ses solutions permettent de déployer un réseau distribué de vidéosurveillance IP, dont les composantes (caméras, serveurs vidéo, archivage, logiciels et systèmes de visionnement) peuvent être géographiquement distribuées.
Tropos Networks (États-Unis) www.tropos.com	Tropos Networks est un chef de file dans les réseaux sans fil à large bande permettant aux clients de déployer une infrastructure IP, notamment pour la vidéosurveillance.

Autres entreprises en vidéosurveillance	
ALTEL (Québec) www.altel.ca	ALTEL conçoit et installe des systèmes de sécurité intégrés dans tous types d'entreprises. Cette compagnie intègre notamment des outils d'identification vidéo avec les systèmes de contrôle d'accès.
Central Vidéo Système (Québec) www.groupecentral.com	Central Vidéo Système est une entreprise de services œuvrant dans l'intégration de systèmes de sécurité électroniques. L'entreprise offre des conseils pour l'intégration de systèmes de contrôle d'accès, de systèmes de surveillance vidéo (caméras) ou de systèmes d'alarme.
Claridion (Québec) www.claridion.com	Claridion est une entreprise spécialisée dans le domaine de la surveillance automatisée des environnements technologiques. L'entreprise a développé un ensemble de solutions et de produits permettant de contrôler les environnements de vidéosurveillance numérique et d'assurer la haute disponibilité, la performance et l'intégrité des équipements et des données.
ENIXUM (Québec) www.enixum.com	ENIXUM offre des équipements et des services en vidéosurveillance IP, en réseautique et en sécurité informatique.
Excellium (Québec) www.excellium.ca	Cette entreprise offre des produits et des solutions de gestion biométrique de l'identité (incluant l'analyse géométrique des visages) et de gestion proactive de la sécurité à plusieurs types de marchés, soit les gouvernements, les corps policiers, les aéroports, les entreprises commerciales et les grands événements.
InfoExpert Outaouais (Québec) www.infoexpertoutaouais.com	Cette entreprise fournit et installe des systèmes informatiques et des caméras pour la surveillance.
Infynia (Québec) www.infynia.com	Infynia développe, déploie et supporte les solutions adaptées à tous les types de besoins en matière de sécurité et d'informatique. Ses services couvrent aussi la vidéosurveillance.
Intelgest (Québec) www.intelgest.com	Intelgest est un intégrateur et un installateur de systèmes de sécurité, dont la vidéosurveillance.
Matrox (Québec) www.matrox.com	Matrox développe des composantes matérielles pour l'affichage graphique multiple destiné aux environnements de sécurité. Sa gamme de produits s'étend des cartes graphiques qui permettent de contrôler les alarmes et d'y répondre à partir d'une station centrale, à des technologies matérielles pour le décodage de plusieurs flux vidéo IP dans différentes résolutions et une variété de formats.

Autres entreprises en vidéosurveillance	
Obzerv (Québec) www.obzerv.com	Obzerv développe et fabrique des systèmes de vision nocturne de haute performance basés sur l'imagerie active à crénelage temporel (<i>gating</i>), optimisé pour la surveillance de courte, moyenne et longue portée. En associant la technologie innovatrice de crénelage spatial (<i>range-gating</i>) aux systèmes de vision nocturne à intensification de lumière, les caméras Obzerv permettent d'augmenter la capacité de voir dans des conditions difficiles associées à la pluie, la neige et au brouillard ; conditions fréquemment rencontrées dans les domaines de surveillance tels que la sécurité côtière, les opérations anti-terroristes, la recherche et sauvetage et plus encore. Ces systèmes permettent aussi aux intervenants de voir à travers les vitres, caractéristique indispensable pour l'observation à l'intérieur des immeubles et des véhicules suspects.
SecurPlus (Québec) www.groupe securplus.com	SecurPlus est une entreprise qui œuvre dans la conception, la vente et l'installation de produits et de systèmes reliés à la sécurité. Ceux-ci incluent notamment les systèmes de surveillance vidéo, traditionnels ou sur réseaux IP.
SGPTI (Québec) www.sgpti.com	SGPTI fournit des services d'intégration de systèmes de vidéosurveillance. Bien que l'entreprise intègre et installe des systèmes traditionnels analogiques, elle se spécialise dans la vidéosurveillance IP. Elle a notamment participé au déploiement des réseaux de vidéosurveillance IP du métro de Montréal, du Quartier DIXTrente et de deux salons de jeux de Loto-Québec.
Smiths Detection Montréal Inc. (Québec) www.smithsdetection.com	Smiths Detection offre des produits de sécurité dans les secteurs civil et militaire. Commercialisant principalement des capteurs pour la détection d'agents chimiques ou biologiques, l'entreprise offre aussi des systèmes de surveillance vidéo.
VideoWave Networks (Québec) www.videowave.ca	VideoWave Networks Inc. est une firme canadienne basée à Saint-Laurent, spécialisée dans la conception de systèmes intelligents de vidéo surveillance visant à optimiser la sécurité des particuliers, des entreprises et agences gouvernementales. L'équipe de concepteurs de VideoWave a conçu le produit VST-OneTrack, un système de tracking avec caméra PTZ, pour lequel VideoWave s'est mérité le prix Octas 2006 dans la catégorie Innovation technologique. Outre ses produits propriétaires, VideoWave propose une gamme complète d'enregistreurs numériques, caméras et serveurs vidéo.
Visio-Soft (Québec) www.visio-soft.com	Visio-soft offre des systèmes de surveillance intégrés, entièrement numériques, sur les protocoles de communications réseaux TCP/IP. L'entreprise détient son propre codec, appelé W1. Elle offre aussi des solutions pour la vidéosurveillance par cellulaire nécessitant une transmission à bas débit.
AdvancedIO (Colombie-Britannique) www.advancedio.com	AdvancedIO vend des produits de connectivité Ethernet gigabit adapté pour le transfert IP, notamment de vidéo, dans les systèmes informatiques à haute performance.
Extreme CCTV (Colombie-Britannique) www.ExtremeCCTV.com	Manufacturier de systèmes de vision nocturne active, à partir d'illumination infrarouge, Extreme CCTV vend ses produits pour la surveillance d'installations critiques, la Défense, la sécurité intérieure, les transports et les sites patrimoniaux.

Autres entreprises en vidéosurveillance	
Micro Video (Ontario) www.microvideo.ca	Micro Video commercialise des caméras miniatures de vidéosurveillance.
Pleora Technologies (Ontario) www.pleora.com	Pleora Technologies fournit des solutions de connectivité Ethernet gigabit pour la vidéosurveillance, la diffusion vidéo et la visionique.
Visual Defence (Ontario, avec bureau à Montréal) www.visualdefence.com	Cette entreprise intègre et installe de l'équipement de vidéosurveillance, tels que caméras, enregistreurs numériques et logiciels d'analytique vidéo.
ADI-Burtek (États-Unis, point de vente au Québec) www.adi-burtek.com	ADI-Burtek est un distributeur de produits électroniques, notamment de vidéosurveillance.
ADT (États-Unis, bureaux au Canada, entreprise de Tyco) www.adt.com	Établi à travers le monde, ADT est l'un des plus grands intégrateurs de systèmes de sécurité. ADT intègre et commercialise les produits de vidéosurveillance de Cisco.
ATEME (France, bureau au Québec) www.ateme.com	ATEME est un manufacturier d'encodeurs et d'enregistreurs vidéo pour la surveillance. Il fournit des solutions de compression, notamment selon les standards MPEG-4 et H.264.
ICX Vision Systems (États-Unis) www.visionsystems.icxt.com	ICx Vision Systems (anciennement PureTech Systems, Inc., division de ICX Technologies) développe PureActiv™, un système pour la surveillance automatisée sur des sites extérieurs. Ce système permet de détecter et suivre les objets, détecter les intrusions, contrôler des caméras, pour générer des alarmes et transmettre les séquences présentant une activité suspecte.
Intrinsa (États-Unis) www.intrinsa.com	Intrinsa vend des solutions de stockage en grappe (<i>cluster storage</i>) offrant des centaines de téraoctets d'espace d'archivage pour les systèmes de gestion vidéo IP. Concurrent direct de Pivot3 ou de fournisseurs de solutions de stockage, tels que EMC et Dell.
Pivot3 (États-Unis) www.pivot3.com	Pivot3 vend des solutions de stockage en grappe (<i>cluster storage</i>) offrant des centaines de téraoctets d'espace d'archivage pour les systèmes de gestion vidéo IP. Concurrent direct de Intrinsa ou de fournisseurs de solutions de stockage, tels que EMC et Dell.
Simplex Grinnell (États-Unis, bureaux au Canada) www.simplexgrinnell.com	Simplex Grinnell vend différents systèmes de sécurité, dont de vidéosurveillance, en intégrant les solutions de partenaires.
Tri-ED (États-Unis, point de vente au Québec) www.tri-ed.com	Tri-ED est un distributeur nord-américain de produits de sécurité et de domotique.

Annexe 4 - Entreprises spécialisées dans la conception de logiciels d'analytique vidéo

Cette section recense les développeurs majeurs de logiciels d'analytique vidéo. Ces produits sont très souvent intégrés dans les logiciels de gestion vidéo d'entreprises partenaires. Elle inclut une brève liste de compagnies spécialisées dans les produits de reconnaissance faciale et de reconnaissance de plaques d'immatriculation.

Entreprise	Description de l'entreprise / produit	Fonctionnalités intelligentes
Organix IT (Québec) www.organixitt.com	Logiciels de vidéosurveillance SVMS qui inclut des fonctionnalités intelligentes. Intègre la technologie de ISS pour la détection et le suivi d'objets, ainsi que la reconnaissance de comportements.	• Détection et suivi d'humains. • Reconnaissance de comportements : bagarre, course, saut par-dessus une guérite, graffiti. • Détection d'objets abandonnés. • Détection de fraude aux points de services. • Monitoring de trafic : accidents, objets sur la chaussée, limites de vitesse enfreintes, congestion, piétons, etc. • Comptage de personnes et détection d'affluence. • Reconnaissance de visages (atteint un taux de précision de 93 %). • Reconnaissance de plaques d'immatriculation (acquisition à 60 km/h).
IntelliView Technologies (Alberta) www.intelliview.ca	Développe et commercialise un système complet d'analytique et de gestion vidéo. L'analyse vidéo est faite dans un DVR.	• Détection d'intrusion dans un périmètre. • Activation de PTZ pour suivi d'objet. • Reconnaissance de plaques d'immatriculation. • Filtrage des fausses alarmes causées par les variations environnementales, telles qu'ombres, reflets et neige. • Création de sommaires vidéo pour condenser les séquences à visionner.

Entreprise	Description de l'entreprise / produit	Fonctionnalités intelligentes
Agent VI (États-Unis) www.agentvi.com	Plateforme logicielle dont l'architecture répartit les traitements entre le serveur et les équipements de périphérie (caméras et encodeurs). Déployée dans plus de 25 pays, dans les principaux secteurs d'application.	- Détection de voitures : stationnement illégal, circulation à contresens, passage de plusieurs voitures sous une seule identification (<i>tailgating</i>). - Détection d'objets suspects ou abandonnés. - Détection et suivi d'individus, détection d'attroupements. - Comportements : Détection d'intrusions, rôdeurs, entrée de deux personnes en même temps à un point de contrôle.
Cernium (États-Unis) www.cernium.com	Suite de produits d'analytique : Perceptrak® (intégré avec Milestone), Cernium Edge™, ExitSentry® (détection de déplacement à contresens dans des aires contrôlées, destiné aux aéroports) et Archerfish™ (solution domestique). Reconnue par Frost & Sullivan à titre d'entreprise nord-américaine émergente de l'année 2008.	- Détection de personnes, d'objets et de véhicules et de leur modèle de mouvement. - Reconnaissance de comportements. - Détection de personnes circulant à contresens.
Intelligent Security Systems (ISS) International (États-Unis) www.isscctv.com	Implantée en Amérique et en Europe, cette entreprise offre une gamme étendue de solutions pour la vidéosurveillance, incluant des modules d'analytique. Intègre les produits de tiers.	- Reconnaissance faciale (précision de 95 %, meilleur système selon l'évaluation du département de la Défense). - Monitoring de trafic. - Reconnaissance d'inscriptions sur les conteneurs. - Reconnaissance de plaques d'immatriculation (capture jusqu'à 150 km/h avec un taux de reconnaissance entre 60 % et 95 %). - Détection de fraudes aux points de service et systèmes de guichets automatiques. - Comptage de personnes.
Intellivid (États-Unis) www.intellivid.com	Développeur d'analytique vidéo spécialisé pour l'industrie du commerce de détail. L'entreprise a été achetée par Tyco, en 2008.	- Surveillance des actifs de valeur et détection de vols. - Détection d'intrusion dans une zone à accès contrôlé. - Suivi de suspects d'une caméra à l'autre. - Analyse des déplacements et comportements des consommateurs. - Monitoring de l'affluence des clients pour permettre d'adapter le service.

Entreprise	Description de l'entreprise / produit	Fonctionnalités intelligentes
Ioimage (Israël) www.ioimage.com	Fondée en 2000, commercialise des encodeurs et des caméras intégrant des fonctions d'analytique vidéo, ainsi qu'un logiciel intelligent de gestion vidéo centralisée.	• Détection d'intrusions : intrusions dans une aire contrôlée, <i>tripwire</i>, violation de périmètre. • Détection d'objet abandonné ou subtilisé. • Détection de rôdeur. • Détection de véhicule stationné. • Activation de caméra PTZ pour suivi d'objet. • Détection d'altération de caméras.
Iomniscient (Australie, bureau à Toronto) www.iomniscient.com	Fondée en 2001, l'entreprise offre une gamme étendue de fonctions analytiques. Elle développe et commercialise une suite logicielle d'analytique vidéo, Genius Range, basée sur un algorithme breveté de détection d'absence de mouvement.	• Détection d'objet abandonné dans une foule. • Détection de vol ou de graffiti/vandalisme dans une foule. • Détection d'objet présentant un contraste très faible. • Gestion de foule et de files d'attentes. • Détection de chutes. • Comptage de personnes et véhicules. • Comportements : détection de rôdeurs, personne courant, objet se déplaçant à contresens. • Détection de course. • Protection de périmètres, détection d'intrusion. • Analyse de vitesse/détection d'excès de vitesse. • Reconnaissance de plaques d'immatriculation.

Entreprise	Description de l'entreprise / produit	Fonctionnalités intelligentes
Mate (Israël) www.mate.co.il (Israël) www.mateusa.net (États-Unis)	Fournit une solution complète d'analytique vidéo pour des analyses centralisées ou en périphérie, selon trois couches : protection du périmètre, protection du site et contrôle d'accès. Mate Cortex est un système de gestion d'analytique vidéo destiné à la gestion d'alarmes provenant de plusieurs périphériques d'analytique vidéo, tels que : • Behavior Watch : Système avancé d'analytique vidéo. • Trigger : Encodeur vidéo analytique permettant d'effectuer des analyses vidéo à partir de la caméra. • iSense : Appareil vidéo de comptage de personnes avec caméra intégrée. • Count Watch : Système de comptage de personnes ou véhicules à partir de la vidéo captée par une caméra placée en hauteur.	• Détection de mouvement. • Détection de trajectoire. • Détection d'objet statique. • Détection de présence dans des zones définies. • Détection d'objets circulant à contresens. • Détection de déplacement ou retrait d'objet. • Analyse de la vitesse d'un objet.
ObjectVideo (États-Unis) www.objectvideo.com	Fondée en 1998, commercialise deux plateformes d'analytique vidéo : ObjectVideo OnBoard, pour l'analytique embarquée dans des périphériques, et ObjectVideo VEW, une application sur serveur. Offre une solution avancée de comptage de personnes (ne nécessite pas de vue de haut). Avec plus de 770 000 canaux d'analyse vidéo vendus dans le monde, ObjectVideo® est le premier fournisseur de logiciel vidéo intelligent.	• Détection, classification et suivi d'objets. • Détection d'intrusion. • Détection de comportements suspects, tels qu'une personne rôdant. • Détection d'objet abandonné ou subtilisé. • Comptage de personnes ou de véhicules applicable, par exemple, à la gestion de file d'attente ou le monitoring de trafic. • Activation de fonctions PTZ pour le suivi d'objet suite à une alarme. • Fonctionnalités de recherche à base de règles.

Entreprise	Description de l'entreprise / produit	Fonctionnalités intelligentes
Verint (État-Unis, bureau au Québec) www.verint.com	Offre une gamme complète de solutions de vidéo IP largement reconnues sur le marché : caméras, encodeurs, enregistreurs intelligents, logiciels de gestion vidéo. La suite de produits Nextiva intègre de l'analytique vidéo embarquée dans les périphériques ou centralisée. Les produits Verint sont déployés à travers le monde, notamment dans 55 aéroports, 30 ports, 2 des 5 plus grands détaillants et dans les organisations gouvernementales.	• Détection d'altérations subies par les caméras • Détection d'intrusion dans des périmètres ou aires contrôlées • Détection de rôdeurs • Détection d'objet abandonné ou subtilisé • Détection de véhicules ou personnes circulant à contresens / excès de vitesse • Mosaïque des vues pour le suivi multi-caméras
Vidient (États-Unis) www.vidient.com	Fondée en 2003, cette entreprise commercialise une technologie initialement développée chez NEC Labs. Smar'Catch, le produit d'analytique de Vidient est notamment intégré dans les systèmes d'Unisys, NEC, et Raytheon	• Détection d'intrusions : personne ou véhicule dans une zone interdite, violation d'un périmètre de sécurité, plusieurs personnes ou véhicules entrant avec la même carte d'accès, intrusion par une sortie, personne passant au-dessus ou au-dessous d'une guérite. • Détections de menaces : rôdeurs, voiture stationnée près d'infrastructures sensibles, objets abandonnés/subtilisés, formation d'attroupements, personnes en surnombre. • Suivi par caméra PTZ activé sur alarme.

Reconnaissance de visages

Entreprise	Description
Animetrics (États-Unis) www.animetrics.com	Animetrics développe des algorithmes permettant de recréer un modèle 3D à partir de deux photos d'un visage. Cette technologie est commercialisée en différents produits, dont Animetric90 permettant la reconnaissance faciale robuste à des rotations de +/- 45°.
Cognitec Systems GmbH (Allemagne) www.cognitec-systems.de	Cognitec commercialise FaceVACS, un logiciel de reconnaissance faciale. L'entreprise développe sa technologie depuis 1995.
Geometrix (États-Unis) www.geometrix.com	Geometrix développe des produits d'identification biométrique combinant reconnaissance 3D et 2D du visage et reconnaissance des empreintes digitales. Sa technologie de reconnaissance faciale combine deux caméras ou plus pour bâtir une forme 3D par triangulation.
L-1 Identity Solutions (États-Unis) www.l1id.com	L-1 Identity Solutions offre des solutions matérielles et logicielles, ainsi que des services, pour les applications d'identification d'individu et de contrôle d'accès. L'entreprise commercialise notamment une plateforme biométrique multi-modale, incluant de la reconnaissance faciale.
Note : D'autres concepteurs de logiciels de reconnaissance faciale peuvent être trouvés sur : http://www.findbiometrics.com/tech-showcases/viewshowcase.php?sc_title=Facial+Recognition&showcase_id=12	

Reconnaissance de plaques d'immatriculation

Entreprise	Produit de lecture de plaque d'immatriculation
Genetec (Québec) www.genetec.com	Commercialise AutoVu : http://www.genetec.com/Francais/Products/Pages/license-plate-recognition.aspx
Adaptive Recognition Hungary (Hongrie) www.anpr.net	Commercialise le produit CARMEN®.
CitySync (Royaume-Uni) www.citysync.co.uk	Développe un logiciel de reconnaissance de plaques d'immatriculation et manufacture des produits matériels reliés.
Hi-Tech Solutions (Israël) www.x.htsol.com	Ligne de produits SeeCar : www.htsol.com/Products/SeeCar.html
INEX/ZAMIR (Israël) www.inexzmir.com	Offre plusieurs produits matériels et logiciels pour différentes applications de reconnaissance de plaques.
LPREditor (France) www.lpreditor.com	Commercialise des systèmes mobiles et fixes pour la reconnaissance de plaques d'immatriculation.

Entreprise	Produit de lecture de plaque d'immatriculation
Milestone (Danemark) www.milestonesys.com	XProtect Analytics - License Plate Recognition : http://www.milestonesys.com/products/value_add_products/video_analytics/license-plate-recognition
Optasia (Singapour) www.singaporegateway.com/optasia/imps.html	IMPS™ : www.singaporegateway.com/optasia/imps.html
Pips Technology (Royaume-Uni) www.pipstechnology.com	Commercialise une gamme complète de produits (caméras, logiciels, accessoires) pour la reconnaissance de plaques d'immatriculation.

ANNEXE 5 - Ressources liées à la vidéosurveillance

Vidéosurveillance	
IP Video Market ipvideomarket.info	Site Internet rassemblant de l'information gratuite sur l'industrie et la technologie de la vidéosurveillance IP.
Video Surveillance www.videosurveillance.com	Site Web dédié à la vidéosurveillance. Présente des nouvelles, des éditoriaux, des blogues, des revues et analyses sur les produits de cette industrie.
Video analytics www.videoanalytics.org	Se positionne comme une ressource Internet neutre sur la technologie d'analytique vidéo et sur les fournisseurs de celle-ci.
Sécurité	
Access Control and Security Systems www.securitysolutions.com	Publication destinée aux entreprises et professionnels dans le domaine de la sécurité, présentant les équipements de sécurité et leurs différentes applications.
ASIS International www.asisonline.org	Rassemblant plus de 36 000 membres à travers le monde, il s'agit de la plus grande association en sécurité. Elle offre plusieurs services à ses membres, tels que la formation, la publication d'un magazine et des services de représentation auprès des entreprises, du gouvernement et des médias.
Canadian Association of Defence and Security Industries (CADSI) www.defenceandsecurity.ca	Association sans but lucratif qui représente les entreprises canadiennes oeuvrant dans le domaine de la défense et la sécurité.
CSO www.csosonline.com	Publie des nouvelles, des analyses et des recherches sur un vaste éventail de sujets : sécurité de l'information , sécurité physique, contrôle d'accès et beaucoup plus.
HS Daily Wire www.hsdailywire.com	Site Web de nouvelles sur le marché de la sécurité intérieure, ainsi que les tendances technologiques s'y rattachant.
ISC365.com www.isc365.com	Visant à rapprocher et informer les professionnels de la sécurité, ce site présente des nouvelles quotidiennes, des formations, un répertoire de produits et des opportunités de maillage.
SDM www.submag.com	Magazine couvrant le marché des vendeurs, intégrateurs, distributeurs et installateurs de produits de sécurité.
Security Industry Association (SIA) www.siaonline.org	Association américaine pour les entreprises en sécurité logique et physique. Elle défend les intérêts de ses membres auprès du gouvernement américain, publie des études de marché, crée des standards favorisant l'intégration, dispense de la formation et commandite des foires commerciales.

Sécurité (suite)	
Security Industry Buyer's Guide www.sibgonline.com	Publié par ASIS International, ce guide recense les produits et les services de l'industrie de la sécurité. Il comprend plus de 3 000 manufacturiers et fournisseurs de produits et services dans ce domaine.
Security Info Watch www.securityinfowatch.com	Site Internet présentant des nouvelles sur l'industrie et le marché de la sécurité.
SourceSecurity.com www.sourcesecurity.com	Guide en ligne pour le secteur de la sécurité.