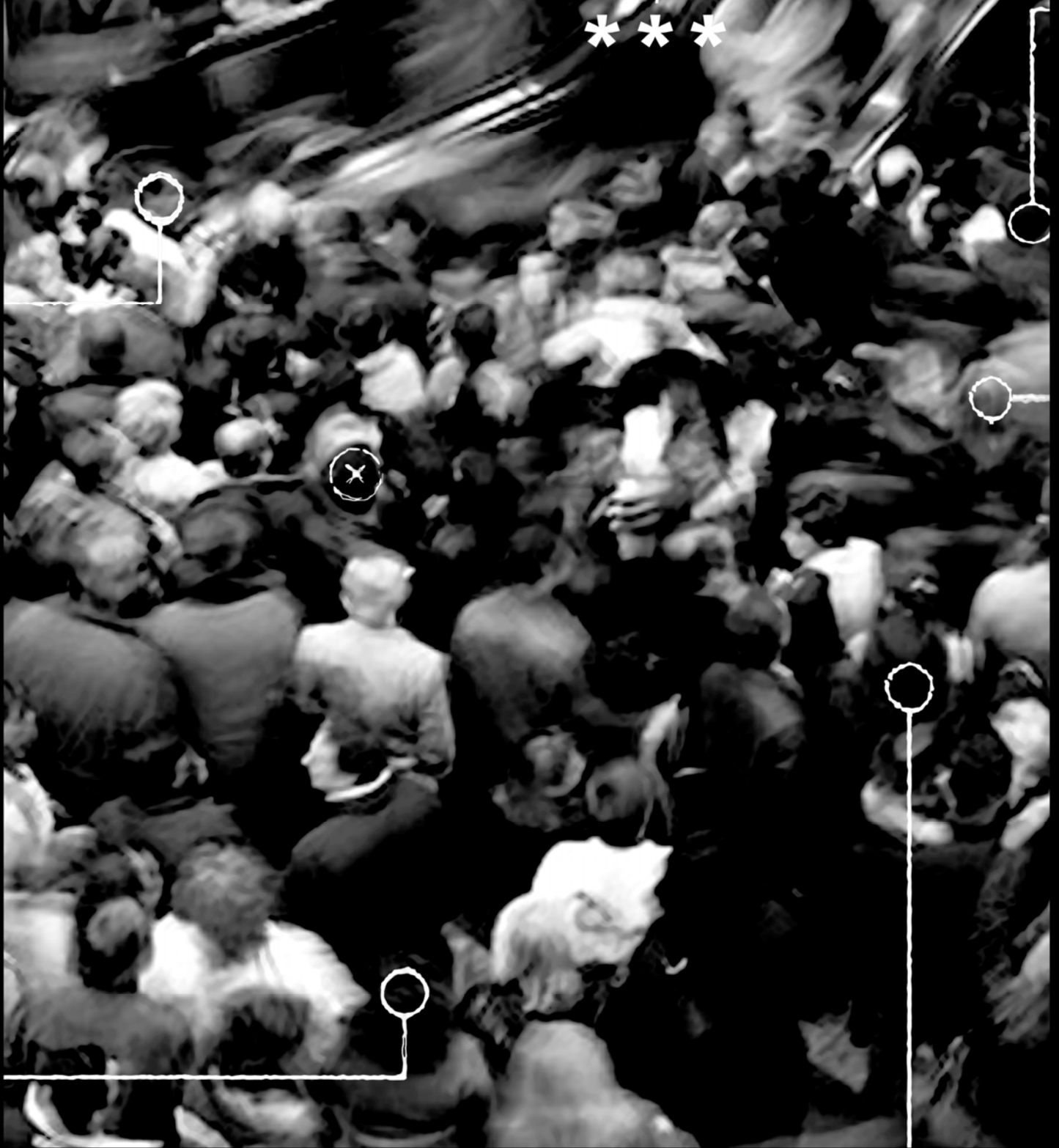


# Dans la mire d'hypervisor

Frédéric Gaillard / Pièces et main d'œuvre

\* \* \*



## DANS LA MIRE D’HYPERVISOR

**A**

**lors que s’accélère le quadrillage de la planète par un arsenal sécuritaire toujours plus performant – caméras, capteurs, puces RFID, drones – certains esprits forts se rassurent encore en dénonçant le gâchis que représentent de tels investissements.**

**“*Trop d’images tuent l’image*”, entend-on : ces mouchards pléthoriques, simple élément de conditionnement de la population, seraient en réalité inopérants du fait même de la gigantesque quantité de données qu’ils génèrent.**

**C’est sous-estimer le lobby militaro-industriel, qui au demeurant ne demande rien d’autre. Dans le secret des centres R&D, on investit sur le véritable enjeu de demain : la mise en œuvre de systèmes centraux intelligents, capables d’analyser les énormes flux générés par les différents équipements, d’en tirer *l’information utile* et de déclencher automatiquement la réponse adaptée. Faisons connaissance avec Hypervisor, dernière *avancée majeure* de la multinationale Thales, lequel annonce en toute simplicité son ambition : donner aux décideurs les moyens d’un contrôle sans faille sur tout et sur tous, et faire entrer le monde dans une nouvelle ère de domination durable.**

*“Nous allons tripler le nombre de caméras de surveillance en France d’ici 2011”* : personne n’a pu échapper au martial mot d’ordre matraqué depuis des mois par Hortefeux et Alliot-Marie, relayés par l’ensemble des trompettes médiatiques du gouvernement. Le Fonds Interministériel de Prévention de la Délinquance a notamment prévu de consacrer en 2009 une enveloppe de 28 millions d’euros (sur un budget de 37) à cette *“priorité absolue”*, qui fera passer de 20 000 à 60 000 le nombre des équipements de vidéosurveillance dans l’Hexagone – encore loin derrière le Royaume-Uni, qui en compterait déjà plus de quatre millions.

Ces réalités assommantes suscitent de bien compréhensibles réflexes de déni dans la population, jusqu’à sa frange la mieux informée. Nouvelle manifestation de la corruption de nos élus par le lobby industriel, le développement vertigineux de la vidéosurveillance ne serait qu’un énième bluff sécuritaire à l’intention du gogo moyen, la gigantesque quantité de données générée rendant impossible toute exploitation opérationnelle des images.

La lecture du site internet du groupe Thales suffit à infirmer cette croyance. La multinationale militaro-sécuritaire vient d’y publier une longue et effarante série de textes<sup>1</sup>, consacrés à une toute nouvelle architecture informatique. Appelée à révolutionner la surveillance, celle-ci est aimablement baptisée Hypervisor.

Dans ce qui suit et sauf indication contraire, toutes les citations en italique sont issues dudit site, dont on ne peut que conseiller la lecture intégrale (pas motivés et âmes sensibles s’abstenir).

.....

*“Hypervisor est certainement l’une des avancées technologiques majeures parmi celles que nous avons identifiées ces dernières années”,* annonce Bruno Nouzille, Vice President Technology for Security Solutions & Services, Thales. *“Nous avons décidé d’investir massivement sur ce concept pour développer une offre qui soit réellement à la pointe.”*

---

<sup>1</sup> < [www.thalesgroup.com](http://www.thalesgroup.com) >, division Sécurité, onglet Thales Hypervisor. Accès direct : < [http://www.thalesgroup.com/Markets/Security/Related\\_Activities/Hypervisor/Thales\\_Hypervisor/?langtype=1036](http://www.thalesgroup.com/Markets/Security/Related_Activities/Hypervisor/Thales_Hypervisor/?langtype=1036) >

Thales, ex-Thomson CSF, “*leader mondial des hautes technologies sur les marchés de l’aéronautique, de l’espace, de la défense, des transports et de la sécurité*”, partenaire privilégié de l’Etat français (son premier actionnaire en 2009 avec 28 % du capital), emploie 68 000 personnes dans 50 pays et a réalisé en 2008 un chiffre d’affaires de 12,7 milliards d’euros. On lui doit depuis un demi-siècle d’innombrables *avancées majeures* dans des domaines comme les technologies d’armement de pointe, l’identification biométrique, le cryptage de données, le contrôle d’accès, dont bénéficient déjà toutes les armées, toutes les polices au monde, pour peu qu’elles soient solvables. Lorsqu’un tel groupe annonce son intention “*d’investir massivement sur (un) concept,*” il est tout indiqué de s’intéresser au concept en question.

Intéressons-nous donc à Hypervisor. Thales livre une vision éclairante des desseins nourris par ces philanthropes quant à notre avenir – disons plutôt “l’avenir”, car nous n’aurons rien à y faire.

Comme dans toute bonne vente, on commencera par un diagnostic – limpide en l’occurrence – du *besoin client* :

*“Au cours de la dernière décennie, le nombre des dispositifs supervisés – caméras, capteurs et équipements contrôlés à distance – a augmenté de façon exponentielle. Dans le même temps, les architectures permettant de les exploiter efficacement peinent à suivre le rythme et les systèmes de supervision ne sont donc pas utilisés au maximum de leur potentiel. Les applications qui contrôlent les équipements sont fréquemment incompatibles entre elles, d’où une perte de complémentarité fonctionnelle. (...) Enfin certaines fonctions – telles que la vidéosurveillance (CCTV<sup>2</sup>) – génèrent une telle quantité de données, qu’il est à l’heure actuelle illusoire d’espérer avoir une vision claire des événements.”*

Or, la vocation de l’industrie sécuritaire est précisément, et plus que jamais, de “*fournir une vision claire des événements*” à ses clients. Mignonne litote explicitée plus loin dans un paragraphe titré “*Contrôle total*” :

*“Dans le domaine de la sécurité urbaine, l’enjeu est d’être pleinement informé de la situation. Il faut pour cela compiler une grande quantité de données remontées de sous-systèmes complexes tels que vidéosurveillance, réseaux de capteurs et systèmes de suivi GPS.”*

---

<sup>2</sup> Close-circuit television – synonyme pour vidéosurveillance.

Ou encore :

*“Pour savoir exactement ce qui se passe en tout point de la cité et mettre en place des actions efficaces, les décideurs ont besoin de croiser des informations issues de multiples sources, d’éliminer les données non pertinentes, (...) pour décider des actions nécessaires et transmettre les instructions dans les meilleurs délais. Ils doivent enfin pouvoir suivre et diriger au plus près les unités présentes sur le terrain en temps réel.”*

Clarifions tout de suite pour les lecteurs distraits : Hypervisor est LA solution à tous ces “défis vitaux”, et bien plus encore. Fin du suspense. Début de l’argumentaire philosophico-technico-commercial. Les tenants du “Total information awareness program” (TIA), devraient apprécier. Poussé par les néo-cons du Département de la défense américain dans la foulée du 11 septembre 2001, ce projet de fichage total des populations, alliant contrôle généralisé de l’internet, identification biométrique, coopération renforcée des banques, compagnies aériennes et autres administrations, s’est heurté fin 2002 aux réticences du Congrès. Un temps rebaptisé “Terrorist information awareness”, le programme est officiellement abandonné – en réalité prudemment saucissonné en plusieurs programmes parallèles, confiés à différentes universités américaines<sup>3</sup> Pour contrôler le monde, il faut de la suite dans les idées. Entendu ce jour à la radio : Nicolas Sarkozy identifie le développement des nanotechnologies comme l’une des deux priorités majeures (avec le numérique) du fameux “grand emprunt national” de 35 milliards d’euros.

.....

Parmi les multiples avatars orwelliens que charrie cette époque, Hypervisor est conçu pour occuper une place bien particulière : celle du-dessus. Cette méta-babasse virtuelle, entièrement basée sur des serveurs web et des codes open source, est présentée successivement comme une “*architecture informatique de nouvelle génération*”, un “*nouvel environnement ouvert pour la gestion de la sécurité et des opérations*”, ou encore une “*solution globale pour la gestion opérationnelle quotidienne comme pour les situations de crise*”.

Ce truc, donc, a la capacité effectivement révolutionnaire d’intégrer, dans un périmètre de “supervision” potentiellement illimité, toutes sortes d’applications, existantes ou à venir, aussi hétérogènes soient-elles, aussi

---

<sup>3</sup> Voir *Terreur et Possession*, par Pièces et Main d’Œuvre, éd. L’Échappée, p.160-162.

éloignées soient-elles. Il permet en outre aux “opérateurs”, via une interface homme-machine (IHM) unique, de “prendre le contrôle” de manière simple et “conviviale”, sur toutes ces applications jusqu’alors disjointes et dotées de règles de commande hétéroclites.

*L’information utile* est extraite en continu, par croisement des données en provenance de toutes les sources. De puissants algorithmes, paramétrables à volonté, permettent de générer des alertes automatiquement. Si le client le souhaite, Hypervisor peut aussi prendre en charge lui-même les opérations pour répondre à un événement donné, “sans aucune intervention humaine”. “Par exemple, avec notre solution, il sera aisé de mettre en place des échanges automatisés entre le module de pilotage du métro, la vidéosurveillance et le système de détection incendie, explique Gérard Basso, product strategy director, urban rail, Thales. De cette façon, (en cas d’incident NdR) on pourra coordonner avec une réactivité et une sécurité maximales des opérations comme l’arrêt des autres trains en station et l’activation des portes pare-feu.”

Autre exemple, dans un paragraphe titré “Prendre le contrôle” :

*“(…) appel d’urgence suite à un accident de la route. Des blessés sont signalés. L’opérateur téléphonique utilise un sous-système dédié pour renseigner l’événement, pendant que l’origine géographique précise de l’appel est automatiquement indiquée sur un plan. Une application de gestion des ressources permet alors à l’opérateur de générer la réponse adaptée et de sélectionner automatiquement les véhicules et les équipes nécessaires. Les ressources mobiles sont suivies par GPS et leurs positions relevées en temps réel sur un système d’information géographique, qui permet aux responsables de juger la situation en un clin d’œil. Valeur ajoutée supplémentaire : Thales Hypervisor permet de prendre la main sur d’autres sous-systèmes comme la signalisation routière, ce qui peut s’avérer précieux par exemple pour faciliter l’accès des équipes de premiers secours.”*

Remplacez “accident de la route” par “attaque terroriste”, “manifestation illégale” ou “attroupement d’individus suspects”. À la fin, mettez juste “forces de l’ordre” à la place de “premiers secours”. Vous verrez, ça fonctionne aussi très bien.

On trouve encore sur le site de nombreux exemples, dans tous les domaines d’application d’Hypervisor : sécurité urbaine bien sûr, mais aussi réseaux de transports en commun, aéroports, pipelines, réseaux d’eau potable,

complexes industriels et autres sites sensibles – de la prison de Fleury-Mérogis au pèlerinage de La Mecque, déjà truffés de mouchards par les soins de Thales et de ses semblables.

L'un des “business cases” les plus avancés est celui de la municipalité de Mexico City :

*“Avec 22 millions d’habitants sur 5 000 kilomètres carrés, Mexico est la troisième agglomération du monde. Thales travaille en partenariat avec le secrétariat d’Etat à la sécurité publique pour rendre plus sûre la vie des citoyens en créant le système de sécurité le plus complet au monde. Il intègre notamment :*

- 8 080 caméras CCTV dont 80 % avec analyse vidéo*
- 380 capteurs de coups de feu*
- 255 caméras à reconnaissance automatique d’immatriculation*
- 180 caméras de surveillance du trafic pour les grands axes*
- 2 centres tactiques de contrôle-commande mobiles*
- 4 drones de reconnaissance aérienne*
- 5 centres C2 (contrôle-commande) régionaux*
- 1 centre national C4I (commande, communication, informatique et intelligence)*
- Un réseau de téléphones d’urgence couvrant toute la ville”*

Où l’on apprend au passage que les technologies de CCTV intelligente incluant de l’analyse vidéo sont appelées à jouer un rôle toujours plus important : *“Elles pourront tout quantifier, depuis la longueur de la file d’attente à un comptoir d’embarquement d’aéroport jusqu’aux rassemblements de foule dangereux dans les rues des villes. Intégrées aux systèmes d’information géographique et aux moyens satellitaires, elles pourraient conduire à une véritable transformation de la sécurité urbaine.”*

Un potentiel encore augmenté par les nouvelles solutions d’analyse vidéo capables de traiter d’énormes volumes d’image vidéo en temps réel, et de déclencher des alarmes automatiquement : *“Ces applications intègrent des algorithmes avancés, qui peuvent être utilisés pour détecter toutes sortes de choses, depuis les objets abandonnés jusqu’aux comportements atypiques, et réalisent des mesures de flux et de densité de foule pour identifier les congestions potentiellement dangereuses dans l’espace public.”*

Ami lecteur, tu sembles un peu pâle. Aurais-tu quelque “comportement atypique” à te reprocher ?

Entre la brique élémentaire (la caméra par exemple) et l’hyper-système global, les systèmes de surveillance sont destinés à s’intégrer les uns dans les autres, du plus simple au plus complexe, à la manière de poupées gigognes. Le Smart Corridor développé par Thales (encore !) fournit un bon exemple d’intégration intermédiaire, à l’échelle d’un couloir d’aéroport. *Lefigaro.fr*<sup>4</sup>, dans un article du 01/12/08, nous y voit déjà :

*“Aéroport de Roissy-Charles-de-Gaulle, 13 h 15. Dans quelques minutes, l’embarquement du vol Air France AF 546 à destination de Washington sera terminé. La routine. Mais alors que les derniers passagers accomplissent les formalités d’inspection et de filtrage, la tension vient de monter brutalement. Sur son écran de contrôle, l’opérateur ne peut avoir aucun doute. L’homme qui vient de passer dans le corridor de détection a manipulé récemment des explosifs et porte une arme sur lui. Une boule dans la gorge, l’agent de sécurité ne quitte pas son écran des yeux. A gauche, une photo biométrique de l’individu et son identité apparaissent. Au centre, sa silhouette informatisée présente une anomalie au niveau du bassin, signalée par un graphique rouge. Signe qu’un objet métallique est porté à la ceinture. A côté, le système de mesure numérique des composants explosifs est à son maximum. Enfin, à droite, les contours du suspect, représentés sous forme de pixels, confirment la présence d’un pistolet automatique dissimulé sous ses vêtements. L’opérateur doit alerter les autorités au plus vite sans semer la panique parmi les autres voyageurs qui poursuivent le contrôle. Heureusement pour lui, il ne s’agit que d’une simulation.*

*En réalité, nous ne sommes pas à Roissy, mais à (Vélizy, NdR), au cœur du laboratoire de la division T3S du centre de recherche du groupe d’électronique et de défense Thales, le Thales Research and Technology (TRT), où est testé actuellement un nouveau système de contrôle des passagers : le Smart Corridor.”*

---

<sup>4</sup> lefigaro.fr, 01/12/08, Cyril Hofstein, “Un couloir hyper-techno pour repérer les terroristes” :

< <http://www.lefigaro.fr/lefigaromagazine/2008/11/29/01006-20081129ARTFIG00665--un-couloir-hyper-techno-pour-reperer-les-terroristes-.php> >



Tout y est, sur les quatre mètres d'un couloir d'embarquement – des caméras intelligentes aux capteurs de matières explosives. Sans oublier le *must* : *“Tous les êtres humains émettent des rayonnements naturels, depuis la température jusqu'aux longueurs d'onde, précise Jean-Luc Zolesio, directeur du comité recherche et technologies de sécurité de Thales. Ce sont ces fréquences spécifiques qui sont enregistrées par notre dispositif.”*

Cette perle a été testée en “temps réel” dans un premier aéroport (non nommé dans l'article) au premier semestre 2009. Mais rassurez-vous : à l'intérieur dudit couloir, on ne sent qu'un léger courant d'air (qui permet de capter les molécules). *“Le Smart Corridor repose sur des fonctions non intrusives et ne produit aucune image détaillée de la silhouette.”* Votre intimité est sauve, si l'on ose dire.

Mais revenons à Hypervisor. L'arsenal des équipements technologiques potentiellement mis en coupe réglée par ses tentacules numériques est, pardon d'insister, illimité. On y retrouve, on l'a vu, toute la gamme des sous-systèmes de surveillance et d'identification. Mais aussi les systèmes de billettique transports publics, tourniquets, portillons d'accès, valideurs de titres. Mais encore les applications “métier” en entreprise : gestion informatisée des ressources humaines et de la paie, planification de la maintenance, messageries et échanges de données sécurisées. Et pourquoi pas les cartes bancaires, les téléphones portables, les systèmes de GPS de véhicules. Tout est possible, on vous dit.

Prenons maintenant cinq secondes pour imaginer quel pouvoir détiendront les maîtres d'Hypervisor – ou d'une technologie concurrente – dans une société où sera achevée la généralisation annoncée des objets communicants, en lien avec le développement fulgurant des nanotechnologies ou des technologies RFID.

.....

*“Nous avons beaucoup d'idées, et un très large champ d'innovation, précise le bien nommé M. Flous, Solution Leader, Thales. Tout va se mettre en mouvement – et continuer à évoluer.”* On ne peut malheureusement pas en douter.

La lecture de la dernière page du site, consacrée aux *“perspectives de la surveillance”*, nous réserve encore quelques beaux gisements de valeur ajoutée. On s'y intéresse notamment au couplage entre l'architecture centrale Hypervisor et de nouvelles applications d'environnements virtuels

développées par Thales pour la simulation et la formation des opérateurs – car, oui, il subsistera quelques hommes-machines pour mettre de l’huile dans les rouages du monde-machine.

*“Nos clients souhaitent pouvoir former leurs opérateurs sans que cela nécessite d’interrompre le service, explique M. Flous. C’est désormais possible grâce à la capacité révolutionnaire de notre solution à lier sa nouvelle architecture de surveillance à nos modules de formation et de simulation. Ce dernier contient tous les protocoles qui interviennent dans les applications de surveillance réelle.*

*Cela signifie que les opérateurs sont formés sur des événements de la vie réelle, au moment où ils ont lieu. En définitive, la seule différence entre la formation et les opérations réelles réside dans le pare-feu numérique qui sépare le monde simulé du monde réel.”*

Voici la condition que l’on nous promet pour demain : depuis leur poste de contrôle hyper-sécurisé, les soldats de la surveillance se forment à leurs procédures d’interventions, l’œil rivé à leurs moniteurs, observant non pas les allées et venues des humains, mais celles, parfaitement synchrones, de leurs clones numériques.

Rapidement, les gains de productivité réalisés par la formation en environnement virtuel devraient justifier l’extension du pare-feu numérique à l’ensemble des activités de surveillance. Car c’est bien ainsi que les décideurs souhaitent voir le cheptel humain dont ils assurent la gestion au travers de la myriade d’yeux de leur hyper-viseur : des *sprites* dépourvus d’expression, de pauvres hères numériques, des amas de pixels muets. Parmi ceux-ci, on recherchera sans relâche les pixels déviants, et on réagira sans l’ombre d’un doute en déclenchant, en temps réel, la procédure adéquate parmi celles proposées par Hypervisor.

On le voit, la réalité dépasse toujours la fiction.

Mais revoilà notre esprit fort, qui tente une dernière salve d’objections – Non, ce n’est pas possible, tout ce délire se base sur l’argumentaire survendeur d’un lobby fanatisé, certainement incapable de mettre en pratique la moitié de ce qu’il avance. Et d’ailleurs, quel gouvernement serait assez fou pour acheter ça ?

Hélas. Thales et consorts (Lockheed Martin, Sagem, Finmeccanica, EADS, BAE Systems, ...) le répètent à longueur de communiqués : leurs avancées

technologiques ne sont dictées que par la lecture et l'anticipation des besoins de leurs marchés. Leurs marchés ce sont nos gouvernants, avec qui ils entretiennent depuis des décennies des relations très étroites, basée sur une immense confiance réciproque et un fort taux de consanguinité. Non, ces gens-là ne sont pas des marchands d'aspirateurs. Ils sont le Pouvoir, au même titre que les Etats dont ils sont les symbiotes mondialisés. Ce que Thales annonce, Thales le fait. Tôt ou tard. Lever les objections juridico-démocratiques fait partie de son cœur de métier.

Sais-tu, lecteur humain, que tu peux d'ores et déjà rencontrer Hypervisor ? Le groupe Thales lui a aménagé un vaste espace de démonstration dans son laboratoire de pointe de Velizy, près de Paris. Mieux vaut cependant motiver ta demande : *“Pour organiser une visite ou étudier la façon dont Hypervisor peut aider votre organisation à atteindre ses objectifs, vous pouvez prendre contact par e-mail : < info.3s@thalesgroup.com >”*

Ce laboratoire, qui constitue le premier centre de recherche dédié à la sécurité en Europe, a été inauguré en 2008 par Jacques Barrot, Vice-Président de la Commission européenne en charge de la Justice, de la Liberté et de la Sécurité. On en revient toujours à ce vieil Orwell : la justice, c'est la domination ; la liberté, c'est la contrainte. La sécurité c'est la guerre.

Citoyen, voici ta laisse.

Et si d'aventure tu montrais les dents, sois sûr que l'hyper-viseur te tiendra en joue.

**Frédéric Gaillard**  
Grenoble, 11 janvier 2010

**Retrouvez ce texte et bien d'autres sur  
[www.piecesetmainoeuvre.com](http://www.piecesetmainoeuvre.com)**

[www.piecesetmaindoeuvre.com](http://www.piecesetmaindoeuvre.com)



# Dans la mire d'hypervisor

“ Alors que s'accélère le quadrillage de la planète par un arsenal sécuritaire toujours plus performant - caméras, capteurs, puces RFID, drones - certains esprits forts se rassurent encore en dénonçant le gâchis que représentent de tels investissements. “*Trop d'images tuent l'image*”, entend-on : ces mouchards pléthoriques, simple élément de conditionnement de la populaion, seraient en réalité inopérants du fait même de la gigantesque quantité de données qu'ils génèrent.

C'est sous-estimer le lobby militaro-industriel,  
qui au demeurant ne demande rien d'autre.”