(Source : Reflets – Titre original « La surveillance numérique : une arme de guerre (presque) assumée »)

Aperçu du salon sur la sécurité intérieure des États et place de la cybersurveillance comme moyen de sécurité

J'ai eu la chance de pouvoir aller à Milipol 2011, salon dit « de la sécurité intérieure des États », qui se déroulait du 18 au 21 octobre porte de Versailles, à Paris. C'est l'un des plus grands regroupements mondiaux de représentants industriels et politiques liés à cette thématique. Hormis la presse, seuls les acteurs de cette sphère y sont en théorie admis. Pas de Monsieur et Madame Tout-le-monde, pas de grand public. Parmi les « personnalités », Marine Le Pen et Claude Guéant y ont apparemment fait une apparition. Parmi les exposants dont le nom parlera peut-être au lecteur, on citera la DGA, Renault Trucks, SigSauer, Flash-Ball, Trovicor et Bull-Amesys. Tous ont une place sur le marché de « la sécurité intérieure des États ».

Ce salon, dont les stands les plus ludiques sont ceux proposant de s'entraîner à viser avec tel fusil mitrailleur ou telle arme de poing, a également donné l'occasion de mesurer l'importance croissante occupée par les technologies de surveillance de masse des flux de communication comme outil de guerre. Une importance très facilement perceptible mais qui semble mal assumée par les fabricants de ces technologies d'espionnage.

Pour cette raison, et du fait que le grand public n'y est pas admis (pourtant l'État, c'est nous, non?), un petit aperçu de ce salon me paraît indispensable. Toutes les photographies de cet article ont été prises lors du salon.

Fais voir ton gros calibre

Première impression: c'est intimidant, et ça fout mal à l'aise. On commence par des tenues spéciales destinées aux militaires et des fusils mitrailleurs flambants neufs, exposés comme des oeuvres d'art. À l'honneur également, des véhicules de police blindés et éventuellement surmontés d'une mitrailleuse. Pour soigner le détail, quelques écrans proposent des animations type jeu vidéo ou mauvais film américain, mettant par exemple en scène les

explosions provoquées par des mitrailleuses d'hélicoptère exposées dans le même stand. Chaque marque rivalise d'ingéniosité pour mettre en valeur ses produits.

C'est beau, non ?

Ce qui occupe une bonne moitié du salon est donc une débauche de haute technologie conçue pour tuer. Une sorte de grand magasin de jouets mais avec de « vrais » jouets, quoi. Comme les petits, on peut venir soupeser, palper et tester le viseur d'une arme dernier cri.

Toute cette haute technologie est le luxe de l'armement. L'exposition de luxe matériel est un levier classique du marketing qui joue sur certains travers du caractère humain pour le pousser à se focaliser sur son envie primaire de posséder un nouvel objet. Milipol, c'est encore plus fort que ça : la plupart de ces objets luxueux ont la particularité d'être conçus pour tuer. Résultat : à l'envie consumériste primaire s'ajoute la poussée de testostérone et le sentiment de puissance qu'on peut observer sur certains mâles venant tâter les armes avec un air satisfait comme si leur virilité s'en trouvait décuplée. Sur les stands les plus soignés, l'arme est même tendue à l'intéressé par une charmante hôtesse, dont le mouvement des doigts sur la crosse ne manquera pas d'éveiller l'inconscient de certains.

Tu la sens ma grosse intelligence ?

Pour parfaire l'ambiance, certains arborent fièrement leur apparat de « représentant de l'ordre public » : tenue du RAID, costume militaire, etc. Si certains de ces représentants sont vraiment fiers de faire partie de la caste virile du salon du fait de la force à laquelle ils ont accès, comment s'étonner de voir certains dégénérés de la BAC perpétrer des excès de violence ou certains CRS s'enorgueillir de la branlée qu'ils ont mis à des Indignés pacifiques ?

J'allais oublier un détail : la place du 9 novembre 1989, face au lieu de l'exposition, était étrangement ornée de dizaines d'affiches publicitaires pour le jeu tout nouveau Battlefield 3.

Un oeil sur les stratégies des États

Faire croire que le salon n'est peuplé que d'écervelés en manque de baston serait toutefois irrespectueux pour les participants ne répondant pas à cette description et omettrait un élément clé : les produits exposés entendent répondre à une stratégie réfléchie et définie par les États, puisqu'ils sont les principaux clients de ces technologies.

Observer les produits mis en avant par les fabricants donne une petite idée des stratégies auxquelles ils répondent. On trouve donc, à ce salon :

beaucoup d'armes de guerre conventionelle anti-infanterie, très puissantes pour certaines (fusils de précision qui t'arrachent un bras en une balle, mitrailleuses pour hélicoptères, armes de poing et armes automatiques en tout genre, robots tout-terrain surmontés d'une mitraillette, …)
des équipements de protection passifs pour les théâtres de guerre (visières et gilets parre-balles) et les violences urbaines (tenues de CRS « blindées », …)
des véhicules, de la moto de police standard BMW au véhicule blindé léger, en passant par le 4×4 de police aux vitres grillagées et surmonté d'une tourelle avec mitrailleuse (j'ai bien dit 4×4 de police, pas militaire, hein)
quelques rares stands sans connotation guerrière, l'un d'eux présentant par exemple un appareil de mesure du taux d'alcoolémie par examen de l'épiderme
pour terminer, les moyens de surveillance des communications électroniques, qui occupent environ un quart du salon à eux seuls.

La sécurité intérieure des États, c'est donc en tout premier lieu la guerre. Mais la guerre contre qui ? Certains éléments rendent la réponse à cette question particulièrement floue. Par exemple, ce 4×4 de police – entité civile censée protéger la population – surmonté d'une arme capable de décimer par dizaines des personnes, civiles elles aussi a priori. Le véhicule blindé aux motifs de camouflage militaires mais avec un fond bleuté pour garder un peu le look « police » me semble également un produit particulièrement pervers.

Il faut que je revoie ma définition du mot "police", je crois...

La frontière semble donc bien poreuse entre baston sanglante et maintien de la sécurité de la population civile… La stratégie des États visant à assurer leur « sécurité intérieure » semble consister à armer davantage les forces de police qu'à se soucier du sort des populations. Et si, à l'instar de l'Égypte, la Tunisie, le Yémen, le Bahrein et la Syrie, c'était les « forces de l'ordre » qui allaient être amenées à représenter la menace la plus dangereuse pour la population ?

Dans ce flou artistique, les technologies d'espionnage de masse des télécommunications

sont loins d'être en reste. L'ambiance sur les stands associés y est même bien plus tendue que dans le reste du salon, surtout lorsque des journalistes y pointent le bout de leur nez.

Des armes de guerre à ne pas dévoiler

Un quart du salon : c'est l'espace occupé par les seuls stands liés aux télécommunications. Parmi eux, j'ai pu observer une dizaine d'exposants de divers pays proposant des solutions d'interception, de stockage et d'analyse de flux réseaux résultants de l'activité humaine. À côté de ces stands où la tension était perceptible, le reste du salon dégageait une ambiance « magasin de jouets » presque relaxante. Pas ou peu d'objets exposés, des regards menaçants à la vue d'un appareil photo, et des représentants particulièrement désagréables avec les journalistes. Pas de doute, ici on propose des produits qui doivent rester cachés et connus uniquement par un public très restreint.

Les brochures publicitaires permettaient tout de même d'apercevoir les caractéristiques des solutions d'interception proposées. Sans surprise, les points quasi-systématiquement mis en avant sont les suivants :

capacité d'interception de flux réseau à très haut débit (j'ai noté le chiffre de 10Gbit/s)
captation de tous les vecteurs usuellement utilisés par les humains pour communiquer (messagerie instantanée, réseaux sociaux, e-mails, webmails, voix sur IP, …)
outils d'analyse et de corrélation des données pour rechercher des individus particuliers ainsi que leurs liens sociaux.

Aucun doute ici non plus : on propose du massif, on met en avant la capacité de passer à l'échelle à la fois en terme de nombre de personnes surveillées et en termes de protocols analysés. Plus concrètement, il est très clair que plus d'une entreprise dans le monde fournit des solutions capables de mettre sur écoute la population d'un pays entier. En plus, certaines d'entre elles ont eu la chance de les tester et les affiner chez les dictateurs d'à côté. Pour changer de Bull-Amesys, qui ne présentait d'ailleurs bizarrement pas son système Eagle, je mentionnerais la société Trovicor, ex-filiale de Nokia-Siemens, apparemment présente dans plusieurs régimes dictatoriaux du Moyen-Orient (cela mériterait d'ailleurs davantage d'investigations).

Ça a le mérite d'être clair : c'est fait pour intercepter des quantités énormes de trafic

Plus effrayant et plus intriguant, une entité italienne nommée « Hacking Team » part d'un constat simple : les données les plus sensibles sont souvent échangées par des canaux chiffrés et sont donc difficiles voire impossibles à intercepter. Qu'à cela ne tienne, Hacking Team propose tout bêtement à ses clients d'installer un logiciel espion sur les machines des personnes dont on souhaite surveiller l'activité. Je n'ai aucun détail technique sur les performances et la furtivité de ce logiciel, mais la brochure vante son indétectabilité par tout type d'anti-virus moderne. C'est une porte de plus qui s'ouvre vers l'installation de logiciels sur des matériels à l'insu des propriétaires. Rappelons-nous que les autorités allemandes ont récemment eu recours à un cheval de troie permettant d'espionner les conversation Skype, et que cette technique est mise en pratique en Chine depuis un bout de temps.

Je n'ai malheureusement ni pu tout retenir ni pu tout photographier. Une énième passe sur ma série de photos me rappelle une autre technologies observée : la localisation tri-

dimensionnelle en temps réel des personnes en grâce à leur téléphone portable.

Extrait de la plaquette publicitaire de Hacking Team

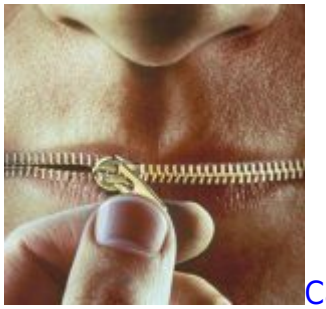
En conclusion, nous sommes en présence de vendeurs de matériel permettant de mettre tout un pays sur écoute et de faire des analyses performantes de ces écoutes, dans un salon amalgamant allègrement matériel de guerre et sécurité des populations civiles dans un flou particulièrement malsain. Et ce salon, censé être autour de la thématique de la sécurité des États (et donc des populations), est interdit au grand public. Enfin, les journalistes, bien qu'autorisés, sont particulièrement mal vus et la plupart des vendeurs de matériel d'interception des flux réseaux restent muets comme des carpes – voire agressifs – face aux questions des journalistes.

Quelques entreprises et quelques oligarchies d'État s'organisent peu à peu pour mettre des millions de gens sur écoute, et le « grand public » ne doit surtout pas le savoir. Je ne comprends pas, moi qui pensais que tout ça était fait pour assurer notre sécurité… Je deviens schizophrène : je suis un citoyen tout ce qu'il y a de plus lambda, et je vais peut-être être surveillé par des armes de guerre tel un ennemi de la population.

À lire également :


France : la justice fait bloquer l’accès au site Copwatch


Procès-baillons : quand les multinationales musèlent lanceurs d’alerte et activistes


Canada : 90% des scientifiques se disent muselés


Division, tension et guerre de religion : la France interdit les prières, les Pays-Bas interdissent la burqa