Forum Européen des Technologies de la Sécurité

Lyon - lundi 8 juillet 2013

Allocution de Manuel VALLS, ministre de l'Intérieur

Seul le prononcé fait foi

Madame la commissaire européenne,

Messieurs les ministres,

Madame la présidente et monsieur le secrétaire général d'Interpol,

Monsieur le sénateur-maire,

Mesdames et messieurs,

Je suis très heureux d'être présent parmi vous, aujourd'hui, pour ouvrir cette première édition du forum « *Technology against crime* », consacré aux relations entre la haute technologie et la sécurité.

Cette initiative – je tiens à en remercier les organisateurs – m'a semblé répondre à un besoin largement ressenti, en France, dans l'Union européenne comme dans le reste du monde, et j'ai donc souhaité que le ministère de l'Intérieur, aux côtés d'Interpol, accorde son parrainage à cet événement.

Nous retrouver à Lyon, et je remercie le sénateur-maire Gérard COLLOMB, n'est pas fortuit : c'est une grande métropole internationale dans beaucoup de domaines, et en particulier dans le domaine de la sécurité avec le siège d'Interpol, la présence de l'Ecole nationale supérieure de police, de l'Institut national de la police scientifique ou bien encore de nombreuses entreprises spécialisées dans les hautes technologies de sécurité. C'est ici, aussi, que des fondateurs de la police technique

et scientifique comme Alexandre LACASSAGNE ou Edmond LOCARD ont entamé leurs travaux il y a un peu plus d'un siècle.

C'est la première fois, à ma connaissance, qu'un tel forum est consacré, au niveau mondial, à une réflexion à la fois prospective et pratique quant aux relations entre la sécurité et la technologie ; et j'ajouterais volontiers les libertés publiques qui doivent constituer notre fil rouge en la matière.

*

Nous sommes au cœur d'une révolution numérique et technologique. Des milliards d'êtres humains sont aujourd'hui instruits, informés, équipés et connectés, formant une société en réseaux.

Ces milliards d'individus, dotés d'outils technologiques puissants, composent une « multitude » puissante et active, qui bouleverse l'ancien ordre économique et social.

Il faut prendre pleinement la mesure de cette révolution, et plonger dans ses conséquences technologiques, industrielles, économiques, sociales, juridiques et politiques.

Le désir de créer, d'innover, de communiquer et de partager n'a jamais rencontré autant de possibilités de passer à l'acte. Positivement bien sûr ! Nos vies, nos interactions, nos créations seront sans doute demain une source déterminante de la valeur et de la croissance de l'économie.

Mais cela a aussi des conséquences majeures en termes de sécurité. Des conséquences qui ne sont pas univoques d'ailleurs comme viennent de souligner Khoo BOON HUI, Michael CHERTOFF et Gille de KERCHOVE ce matin au cours de vos débats.

Les technologies font, en effet, naître de nouveaux risques, il est temps d'en prendre toute la mesure: cybercriminalité, détournement des identités, diffusion de messages de haines ou de radicalisation, piratage des systèmes d'information dans la perspective de détruire, de paralyser, d'affaiblir des Etats ou des organisations Ils sont aujourd'hui particulièrement vulnérables, face aux interceptions sauvages de communications privées – notamment du fait du *cloud-computing* mal maîtrisé ou mal sécurisé – et aux stratégies d'intrusion très offensives dans les réseaux, soit depuis l'extérieur, soit par des dispositifs de captation de données implantés à l'intérieur des entreprises ou des organisations.

L'ampleur et la rapidité de ces attaques peuvent causer des préjudices inestimables, capables de compromettre la survie même de ces Etats ou ces organisations. Le visage des criminels a aussi changé en prenant de plus en plus souvent celui du technicien invisible et spécialisé et qui agit sans se soucier des frontières.

Cette nouvelle donne nous conduit donc à revoir en profondeur nos modes d'action et nos organisations. Elle nous pousse aussi à nous appuyer de façon raisonnée sur la technologie pour trouver les réponses ou du moins les outils permettant de relever ces nouveaux défis. Les fonctions de sécurité informatique sont donc aujourd'hui vitales pour les Etats comme les entreprises qui doivent développer en interne une culture de la sécurité informatique.

Biométrie, cryptographie, optronique, vidéo-protection, caméras miniatures, traitement de l'information de masse, communication spatiale, acoustique, ou encore drones, apportent des réponses opérationnelles aux besoins des services de sécurité intérieure. Ils apporteront plus encore demain l'essentiel des marges d'amélioration qualitatives et quantitatives de l'offre de sécurité.

Le ministère de l'Intérieur français a su prendre le virage technologique en développant ses capacités : dans le domaine de la biométrie, avec les fichiers FAED

et FNAEG ; dans le domaine de la vidéo-protection avec l'appui aux collectivités locales et les entreprises publiques et privées ; dans le traitement automatisé de données avec, par exemple, le développement de la lecture automatique des plaques d'immatriculation (le système LAPI).

Plus récemment, nous avons mis en service un nouveau système de rapprochement criminel, TAJ, qui rassemble les procédures des services de police et de gendarmerie. Il contient une base d'images de 5 millions de mis en cause et un moteur de rapprochement qui a déjà permis de résoudre de nombreux crimes.

Si nous ne voulons pas subir le changement technologique mais au contraire bénéficier de l'innovation de nos entreprises, nous devons donc continuer à l'intégrer dans nos stratégies de sécurité.

Je ne suis cependant pas de ceux qui considèrent que demain, les techniques, aussi puissantes et sophistiquées soient elles, pourront remplacer le travail de l'Homme, surtout dans le domaine de la sécurité.

Leur développement est un facteur de progrès et d'efficacité considérable pour les forces de l'ordre. Mais les techniques (ADN, biométrie, …) ne seront d'aucune utilité sans l'expérience du policier ou du gendarme qui exploite l'outil ; il devra au préalable avoir été formé à leur emploi. Formé aussi à exercer sa capacité de discernement dans l'exploitation, le tri, l'analyse, l'interprétation des données fournies qui devront être mises au regard de la connaissance du terrain. La dimension humaine, la présence sur le terrain, resteront donc des axes majeurs de l'action policière. Dans les domaines de la sécurité publique, de la lutte contre la criminalité organisée, de l'antiterrorisme, du renseignement,…

Mais ces technologies nouvelles apportent aussi de nouvelles réponses pour protéger les femmes et les hommes qui interviennent, souvent dans des situations

dangereuses : à cet égard, la géolocalisation des équipages ou la vidéo embarquée, comme j'ai pu récemment les voir à New York, constituent des progrès majeurs.

Nous devons aussi intégrer ces technologies avec le souci constant d'un équilibre entre l'amélioration de la sécurité de chacun et le respect des libertés individuelles. Pour protéger leur population, tous les Etats ont besoin d'accéder à certaines communications électroniques, aussi bien en matière de renseignement que de poursuites judiciaires. Ils doivent pouvoir le faire en fonction de ce qu'est aujourd'hui la réalité technique de l'internet. Mais l'exploitation des métadonnées ou des contenus n'est légitime que si elle se rapporte à des finalités de sécurité bien circonscrites : lutte contre le terrorisme et la criminalité organisée ou encore protection des intérêts fondamentaux des Etats. Et l'accès aux données doit s'opérer par ciblage des individus ou groupes qui présentent une menace réelle, sous le contrôle d'une instance indépendante garantissant le respect de ces finalités et de ce ciblage…Bref, le déploiement de tout nouvel outil doit inclure dès le départ une réflexion sur les garanties, juridiques ou techniques, qui peuvent être apportées au respect des libertés individuelles. C'est une condition indispensable pour que ces outils technologiques soient acceptés socialement, et donc efficaces.

L'actualité qui a posé un vrai problème de confiance entre Etats-Unis et partenaires, mais aussi pour les usagers des services, nous montre par ailleurs la nécessité d'une entière vigilance sur la protection des données personnelles et le respect des libertés publiques. Notre pays a très tôt attiré l'attention de ses partenaires sur la grande sensibilité de ces questions. Alors qu'un règlement sur les données personnelles et une directive sur la protection des données applicables aux fonctions souveraines sont en cours de négociation à Bruxelles, nous demandons à la commission européenne d'être particulièrement vigilante sur ce sujet. Aucun nivellement par le bas n'est acceptable. Nous souhaitons que la législation s'applique à toutes les sociétés qui fournissent leurs services en Europe et que tous

les citoyens puissent avoir la garantie de pouvoir s'adresser en toutes circonstances à une autorité de protection compétente dans leur pays.

*

La France a la chance de disposer de forces de l'ordre dont la compétence et le professionnalisme sont reconnus bien au-delà de nos frontières ; je pense que beaucoup de ministres présents ici, et je les en remercie, pourront en attester.

Elle a aussi la chance de disposer d'un tissu industriel dynamique et à la pointe de l'innovation dans le domaine des industries de sécurité.

Enfin, elle a fait le choix de soutenir sans réserve la recherche et l'innovation.

Je crois qu'elle dispose donc des atouts indispensables pour réaliser un mariage harmonieux, que j'appelle de mes vœux, entre l'innovation technologique et la sécurité.

Des échanges existent entre l'ensemble de ces acteurs. Mais avec le président de la République, nous avons fait le constat d'une insuffisante structuration de la filière des industries de sécurité alors que les enjeux de compétitivité et de sécurité sont considérables.

De compétitivité, tout d'abord, avec un chiffre d'affaires estimé à 10 milliards d'euros, en croissance annuelle de 7% et 50 000 emplois travaillant principalement à l'export dans des entreprises leaders dans le monde, présentes ici, que je salue, mais aussi dans des PME dynamiques.

De sécurité aussi naturellement, je l'ai souligné au début de mon propos.

Les constats ont été posés et sont aujourd'hui largement partagés.

L'expression des besoins est insuffisamment claire et fédérée de la part des donneurs d'ordre. Les pouvoirs publics ont naturellement leur part de responsabilité… Malgré des initiatives comme celle du réseau des services de

technologies de sécurité au niveau européen, ENLETS, prises sous la présidence française de l'union européenne, le travail d'expression de besoin reste encore largement balbutiant.

De leur côté les industriels expriment légitimement des réticences pour se lancer dans le développement d'outils, en mobilisant des fonds propres importants, pour lesquels les débouchés sont incertains.

La structuration de la filière a donc vocation à rompre ce cercle vicieux, pénalisant pour tous, pouvoirs publics comme industriels.

Il faut donc créer un climat de confiance comme soulignait, Gille de KERCHOVE.

Je me réjouis d'ores et déjà de la création du conseil des industries de la confiance et de la sécurité, le CICS, par les quatre groupements fondateurs que sont la FIEEC, le GICAN, le GICAT et le GIFAS. Il a vocation à accueillir et informer largement tous les acteurs industriels grands et petits. Les PME sont d'ailleurs au cœur de notre réflexion car porteuses d'innovation et aussi d'exportation, vers d'autres pays, et ils sont nombreux, ayant les mêmes besoins.

Nous devons maintenant aller plus loin avec la création du comité de filière prévu dans le récent Livre blanc de la défense et de la sécurité nationale.

Il sera installé à la rentrée par le Premier ministre, sa charte de création est aujourd'hui stabilisée.

Il aura pour mission de développer une vision prospective des besoins, d'identifier des technologies critiques et les domaines sur lesquels une action concertée des industriels, des organismes de recherche et des pouvoirs publics est indispensable, ou bien encore de mobiliser des financements et de développer une politique de soutien à l'exportation que je veux personnellement soutenir

Pour ce qui concerne plus particulièrement le ministère de l'Intérieur, j'ai d'ores et déjà identifié trois défis majeurs pour les prochaines années :

- ✓ La modernisation des réseaux de radiocommunication avec l'intégration de l'image au–delà de la transmission des seules données vocales ;
- ✓ Le déploiement d'une nouvelle génération de vidéoprotection intégrant l'intelligence artificielle et les moyens d'exploitation rapide de très gros volumes d'image ;
- ✓ La modernisation, enfin, des équipements de protection des forces de sécurité qui devront, demain, intégrer de nouveaux matériaux, des capteurs intelligents et des moyens de communication.

Bien sûr nous ne pourrons pas tout faire demain. Je sais les ressources budgétaires dont dispose mon ministère et les choix que nous devons faire dans la politique de sérieux budgétaire voulue par le Gouvernement. Mais rien ne nous interdit de faire preuve d'imagination, d'inventivité et même d'audace pour penser aujourd'hui les forces de sécurité des dix ou vingt prochaines années.

C'est aujourd'hui que nous préparons nos résultats de demain. Je souhaite que ce forum puisse, pour la France comme pour les autres pays représentés ici, y contribuer activement.

Je vous remercie.

***