Discours de M. Bernard Cazeneuve, Ministre de l'Intérieur

Forum international de la cybersécurité

Lille – 26 janvier 2016

SEUL LE PRONONCE FAIT FOI

Monsieur le Ministre, cher John HAYES (*Secrétaire d'Etat à la Sécurité*),

Monsieur le Préfet,

Madame la Maire de Lille,

Mesdames et Messieurs les élus,

Monsieur le Directeur général de la Gendarmerie nationale, mon Général,

Mesdames et Messieurs,

Je suis très heureux de pouvoir m'exprimer devant vous, à l'occasion de cette 8e édition du Forum international de la cybersécurité (FIC). Au fil des années, cette manifestation s'est en effet imposée comme un rendez-vous incontournable pour toutes celles et ceux qui travaillent dans le domaine hautement stratégique de la cybersécurité, et je veux commencer par saluer l'ensemble des organisateurs, la Gendarmerie nationale, bien sûr, qui, dès 2007, a été à l'origine de la création du FIC, ainsi que le conseil régional et les sociétés CEIS et Euratechnologies avec qui elle l'organise désormais en partenariat.

L'intérêt du public ne faiblit pas, si j'en juge par le nombre de visiteurs, sensibles à la diversité et à la qualité des intervenants. Plus que jamais, le FIC propose aux experts et aux décideurs que vous êtes un espace d'échanges et de réflexions d'une très grande richesse.

Je me réjouis également de la présence parmi nous aujourd'hui de M. John HAYES, Secrétaire d'Etat à la sécurité auprès de Mme Theresa MAY, ministre de l'Intérieur britannique.

Je le disais déjà l'année dernière devant vous : nous sommes aujourd'hui confrontés à des défis de sécurité considérables qui exigent une riposte commune, à la fois européenne et internationale. **Ainsi, face au terrorisme, il nous faut poursuivre les efforts communs que nous conduisons depuis plusieurs derniers mois, avec la plus grande détermination.**

En 2015, la France elle-même a été très durement touchée par la barbarie terroriste. Jamais, jusqu'alors, nous n'avions connu sur notre sol des attaques terroristes d'une telle nature et d'une telle ampleur. A cet égard, je veux à nouveau rendre hommage à l'ensemble des forces de sécurité qui, depuis de nombreux mois, se mobilisent, sans ménager leur temps ni leur énergie, pour protéger les Français et défendre nos libertés fondamentales. Nous savons qu'en 2016 la menace sera tout aussi élevée et qu'il nous faudra par là même continuer à faire preuve d'une vigilance et d'un engagement de chaque instant.

Le combat contre le terrorisme se livre également dans le cyberespace. L'organisation DAESH se sert en effet d'Internet et des réseaux sociaux comme de puissants vecteurs de propagande et surtout de recrutement. Nous savons aujourd'hui que la plupart des néo-djihadistes qui ont rejoint ou qui cherchent à rejoindre la Syrie ou l'Irak se sont radicalisés sur Internet. Le caractère inédit et la force réticulaire de nos ennemis résident dans le croisement – certes fortuit, mais dont ils ont su tirer le meilleur parti – entre deux phénomènes concomitants : une évolution stratégique d'une part – l'avènement d'un terrorisme de proximité qui recrute ses activistes dans les sociétés mêmes qu'il entend frapper – et une évolution technologique d'autre part, le développement à partir du milieu des années 2000 de l'Internet 2.0 qui permet la constitution de communautés numériques, lesquelles peuvent représenter autant de lieux où se structure l'identité des individus qui les fréquentent.

Si vous me permettez de plagier une formule célèbre, je dirais, pour résumer, que le néo-djihadisme, c'est la ceinture d'explosifs plus les réseaux sociaux.

Face à cela, notre objectif consiste à entraver l'action et la diffusion de la propagande terroriste. Car, si nous agissons sans relâche pour empêcher la commission d'actes terroristes, il est également nécessaire, au-delà de ce volet sécuritaire, que nous intervenions en amont, notamment sur Internet, pour briser les « continuums de radicalisation » qui peuvent conduire à un passage à l'acte violent.

1. C'est la raison pour laquelle nous nous sommes dotés, depuis plus d'un an, avec l'adoption de la loi antiterroriste de novembre 2014, puis de la loi sur le renseignement de juillet 2015, des moyens juridiques nécessaires.

Dès la publication, en février dernier, des décrets d'application de la loi du 13 novembre 2014, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication a ainsi mis en œuvre les procédures de retrait et de déréférencement de contenus illicites par les moteurs de recherche sur Internet, et, le cas échéant, de blocage des sites qui n'avaient pas procédé au retrait. L'année dernière, nous avons traité plus de 1 000 demandes de retrait et de déréférencement, et 283 blocages de sites ont été réalisés.

Par ailleurs, sur les 188 000 signalements reçus en 2015 par la plateforme PHAROS exploitée par les services de police et les unités de gendarmerie, près de 32 000 concernent des contenus de propagande ou d'apologie du terrorisme, dont une grande partie ont été reçus dans les jours qui ont suivi les attentats du mois de janvier. Si ce phénomène ne s'est pas reproduit avec une telle ampleur en novembre dernier, il n'en illustre pas moins l'influence et la malignité de nos ennemis.

Les procédures que nous avons mises en place ont donc d'ores et déjà prouvé leur efficacité : c'est la raison pour laquelle nous devons les généraliser à l'échelle européenne. J'ai ainsi défendu la mise en œuvre par la Commission européenne, depuis le 1er juillet dernier, d'un dispositif analogue à celui que nous avons mis en place en France : « l'Unité européenne de référencement de l'Internet », susceptible de décupler considérablement notre force de frappe et faciliter ainsi notre travail de repérage, et le cas échéant de suppression, des contenus illicites sur Internet et sur les réseaux sociaux.

2. Plus largement, comme je l'ai répété en maintes occasions, j'ai la conviction que, pour vaincre la menace djihadiste, il ne faut pas seulement l'unité nationale et l'union des démocraties, il faut aussi la coopération des pouvoirs publics avec les acteurs de la société numérique dans laquelle nous vivons.

A cet égard, je constate que, depuis le début de l'année 2015, près de 90 procédures judiciaires visant des activités terroristes ont pu être initiées sur la base de signalements PHAROS, grâce aux réponses transmises par les opérateurs aux réquisitions des services de police et des unités de gendarmerie.

Les attentats du 13 novembre dernier ont été l'occasion de faire la démonstration de l'aide précieuse que les grands opérateurs de l'Internet pouvaient nous apporter en situation de crise majeure. Des services ont été mis en place spontanément sur les réseaux sociaux, qui ont permis à des millions de citoyens de se signaler auprès de leurs proches pour les rassurer. Dans les jours qui ont suivi, ils ont aussi constitué un puissant vecteur d'expression de la solidarité nationale, et même internationale.

Je veux donc remercier aujourd'hui les opérateurs pour leur mobilisation à nos côtés en ces heures tragiques pour le pays. Je leur suis également reconnaissant de la promptitude et de la pertinence avec lesquelles ils répondent aux demandes que leur soumettent régulièrement les services du ministère de l'Intérieur. Nous avons donc su mettre en place une coopération vertueuse qu'il nous faut encourager, car, contre le terrorisme, nous avons besoin de tous les talents, de toutes les énergies et de toutes les responsabilités.

C'est la raison pour laquelle, voici maintenant un peu moins d'un an, je me suis rendu outre-Atlantique, en Californie, pour y rencontrer les représentants des grands opérateurs du numérique afin d'explorer avec eux les voies d'une coopération renforcée face à la menace terroriste. Nous sommes ainsi parvenus, dans le respect du droit existant, à nous mettre d'accord sur une plateforme de bonnes pratiques, que nous avons collectivement adoptée, le 23 avril dernier, lors d'une réunion au ministère de l'Intérieur.

Le principe en est simple.

Notre premier objectif a consisté à améliorer le contenu des demandes que nous adressons aux opérateurs, qu'il s'agisse de demandes de retrait de contenus ou bien de demandes concernant des enquêtes en cours. Nous avons adapté nos logiciels et nos circuits de validation pour tenir compte des besoins exprimés par les opérateurs. Avec eux, nous avons formé au bon usage de ces nouvelles procédures les formateurs numériques de la police et de la gendarmerie.

Réciproquement, au sein des grandes entreprises du Net, la tâche des services en charge des obligations légales a été simplifiée. Ces services sont désormais plus en mesure d'assurer un traitement spécifique de nos demandes ainsi « labellisées ».

Cet accord a marqué le début d'un partenariat particulièrement fructueux, qui se développe à travers le « groupe de contact permanent », animé par le préfet Jean-Yves LATOURNERIE, à qui j'ai par ailleurs, comme vous le savez, confié la mission de piloter notre dispositif de lutte contre les cybermenaces. Je tiens à cet égard à saluer le travail important qu'il a d'ores et déjà réalisé pour mettre en œuvre le plan ministériel de lutte contre les cybermenaces que nous avons adopté dès 2014.

Depuis un an, le préfet Jean-Yves LATOURNERIE, dont je salue l'action, conduit à ma demande une mission de préfiguration d'une délégation ministérielle à la lutte contre les cybermenaces. Son remarquable travail, sur lequel nous nous entretiendrons dans les prochains jours, me permettra de fixer les conditions dans lesquelles pourra être définitivement constituée cette délégation qui nous permettra de mieux coordonner l'action que nous menons contre toutes les cybermenaces.

Le premier objectif assigné au « groupe de contact permanent », qui réunit régulièrement les opérateurs et les représentants du ministère de l'Intérieur, du ministère de la Justice et du secrétariat d'État au Numérique, est donc en passe d'être atteint : il constitue désormais une instance de dialogue libre et efficace, fondée sur la confiance mutuelle, entre l'Etat et les opérateurs.

La France a donc été pionnière en la matière. Aujourd'hui, les Etats-Unis ont à leur tour affirmé vouloir travailler avec les opérateurs pour contrecarrer l'activité des terroristes sur Internet. Notre audace a payé, et aujourd'hui nous faisons école, ce dont je me réjouis, car c'est ainsi que nous pourrons contribuer à garantir au mieux la sécurité collective.

3. Enfin, outre le renforcement de notre arsenal juridique et la mise en œuvre de coopérations inédites, nous avons également renforcé, depuis l'adoption en janvier dernier du plan de lutte antiterroriste (PLAT), l'ensemble des moyens humains, matériels et technologiques dont dispose le ministère pour lutter contre toutes les cybermenaces.

A titre d'exemple, la sous-direction de la lutte contre la cybercriminalité, qui intègre la plate-forme PHAROS et l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, a vu ses effectifs augmenter de façon significative : elle compte désormais 100 personnels (depuis le 1er janvier), contre 70 voici un an.

De même, au sein de la Gendarmerie nationale, le Centre de lutte contre les criminalités numériques (C3N) et l'Institut de recherche criminelle (IRCGN) rassemblent 60 enquêteurs de haut niveau placés à la tête du réseau CYBERGEND qui regroupe désormais plus de 2 000 enquêteurs, répartis sur l'ensemble du territoire national.

Cet effort de renforcement, qui se poursuivra dans les mois à venir, s'inscrit dans un cadre plus large : le **plan de modernisation pour la sécurité** dont j'ai souhaité la mise en œuvre pour le ministère de l'Intérieur. Ce plan vise à moderniser les moyens des forces de sécurité, mais aussi à proposer de nouveaux services numériques à nos concitoyens. Il représente un budget très conséquent : 108 millions d'euros investis sur trois ans, de 2015 à 2017.

J'attache une extrême importance à ce que ces projets soient conçus dans une démarche collaborative impliquant tous les acteurs ministériels – particulièrement les forces de police et de gendarmerie – voire interministériels. À l'heure de la révolution numérique, l'intégration numérique ne doit plus se heurter au

cloisonnement des forces. Au moment où, face aux défis auxquels nous sommes confrontés, la coopération internationale et le partenariat avec les grands acteurs privés sont ô combien nécessaires, il est plus que temps de faire tomber, au sein même de notre maison, les cloisons internes qui n'ont plus lieu d'être.

C'est dans cet esprit que travaille la délégation ministérielle aux industries de sécurité, confiée à Thierry DELVILLE, qui constitue pour ces dernières un point d'entrée unique et un interlocuteur bien identifié. Je souhaite à cet égard que les décisions annoncées lors de la réunion du Comité de la filière des industries de sécurité (COFIS), le 1er décembre dernier, trouvent rapidement une application concrète, notamment pour faciliter les coopérations entre l'Etat et les industriels en cas de crise.

Par ailleurs, je peux vous garantir que la France soutiendra toute initiative de la Commission européenne et des acteurs concernés pour développer un marché européen de taille critique suffisante.

S'agissant du plan de modernisation proprement dit, je veux citer en particulier **deux défis majeurs d'ores et déjà engagés**.

Le premier concerne la mobilité des forces. Piloté par les directions générales de la police nationale et la gendarmerie nationale, et conduit techniquement par le service des technologies et des systèmes d'information de la sécurité intérieure, il a bénéficié également du concours technique de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) pour la solution de transmission sécurisée. Il s'agit de doter les policiers et les gendarmes d'un outil sécurisé de mobilité opérationnelle, qui leur permette de disposer des informations nécessaires à l'accomplissement de leur mission et de conduire un certain nombre de procédures depuis le terrain. L'expérimentation NEOGEND menée par la gendarmerie dans le département du Nord depuis le mois de septembre 2015, avec 1 000 équipements individuels de ce type, démontre la pertinence et l'efficacité du système. Après une seconde phase d'expérimentation à plus large échelle dans le courant de cette année, plus de 60 000 équipements de mobilité opérationnelle auront été déployés, d'ici la fin 2017, sur l'ensemble du territoire.

Le second défi concerne l'utilisation d'outils décisionnels. Il s'agit d'exploiter, dans le strict respect des libertés individuelles, les grands volumes de données disponibles et accessibles, dans le cadre de l'open data notamment ou bien dans les systèmes d'information propres au ministère. Ce projet est mené par le pôle judiciaire de la gendarmerie nationale, que j'ai inauguré en 2015 à Pontoise, et notamment par le service central du renseignement criminel.

Si la lutte contre le terrorisme est une priorité absolue, le ministère de l'Intérieur ne s'en consacre pas moins à la lutte contre toutes les formes de criminalité numérique. Cet effort s'inscrit dans la « stratégie nationale de sécurité pour le numérique » présentée le 16 octobre dernier par le Premier ministre. J'ai souhaité que le ministère de l'intérieur y joue un rôle actif et soit force de proposition dans l'élaboration de cette nouvelle stratégie.

J'ai tenu en particulier à ce que **l'accueil des victimes de cyber malveillance** – notamment les particuliers et les petites et moyennes entreprises, qui ne disposent pas toujours des compétences et des moyens nécessaires – soit significativement amélioré sur l'ensemble du territoire.

En la matière, l'information des victimes est une véritable nécessité.

Un groupe de travail présidé conjointement par le préfet LATOURNERIE et le directeur général de l'ANSSI a présenté un certain nombre de propositions. Je souhaite que plusieurs d'entre elles soient mises en œuvre avant la fin du mois de juin, dans au moins une région pilote. Elles porteront sur l'identification d'un réseau de partenaires locaux susceptibles d'accompagner concrètement les victimes. En particulier, les entreprises qui constituent des cibles récurrentes ou prioritaires d'actes de cyber-malveillance doivent bénéficier d'une meilleure information sur les interlocuteurs à leur disposition, notamment les services d'enquête spécialisés de la police et de la gendarmerie. En mobilisant, aux côtés des acteurs locaux, les réseaux territoriaux de l'Etat, je souhaite donc que nous gagnions en efficacité dans la transmission des messages de prévention et dans l'assistance aux victimes.

Outre le renforcement de nos dispositifs d'information, l'autre priorité qui nous mobilise réside dans la modernisation et l'adaptation de notre cadre juridique et réglementaire. Une telle exigence, valable contre le terrorisme, l'est aussi contre les autres formes de cybercriminalité. L'évolution rapide et la diversification des menaces nous imposent en effet de donner aux enquêteurs de nouveaux moyens d'investigation. Je pense par exemple à la possibilité d'enquêter sous pseudonyme, récemment étendue aux infractions cyber.

Nous devons également adapter nos procédures et nos outils juridiques traditionnels au caractère mondialisé et ubiquitaire de la cybercriminalité. Les procédures d'entraide judiciaire doivent ainsi être simplifiées afin de permettre aux enquêteurs de recueillir plus rapidement auprès des acteurs numériques étrangers les données nécessaires à la poursuite des investigations.

Enfin, le projet de loi renforçant d'une part la lutte contre le crime organisé et son financement, et d'autre part l'efficacité et les garanties de la procédure pénale, qui sera présenté au Conseil des ministres le 3 février, intégrera des dispositions visant à faciliter le travail des enquêteurs, notamment dans le cas d'enquêtes complexes telles que celles qui concernent le cyberespace. En particulier, l'adoption d'un nouveau critère de compétence territoriale permettra désormais à la justice française de connaître des faits commis en dehors du territoire national, dès lors que la victime de cyber malveillance réside France.

Mesdames et Messieurs, chacun d'entre nous sait qu'aujourd'hui le destin de notre pays se joue pour une large part dans la transition numérique. Parce que notre sécurité collective se défend aussi dans le cyberespace, je veux tous vous remercier, vous qui participez au Forum international de la cybersécurité, pour la contribution décisive que vous apportez à la lutte que nous menons collectivement contre toutes les cybermenaces.

Je vous remercie.