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

Forum international de la cybersécurité

Lille – 20 janvier 2015

Monsieur le Ministre, cher Thomas de Maizière,

Monsieur le Préfet,

Mesdames et Messieurs les élus,

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

Mesdames, Messieurs, chers amis,

Je suis très heureux d'ouvrir aujourd'hui les travaux de la 7ème édition du Forum international de la cybersécurité. Un lien naturel et durable unit en effet le ministère de l'Intérieur à cette manifestation, lancée à l'initiative de la

Seul le prononcé fait foi

Gendarmerie nationale en 2007 et aujourd'hui organisée en partenariat avec le Conseil régional du Nord Pas de Calais et la société CEIS.

La diversité et la qualité des intervenants et des participants à cette nouvelle édition du FIC confirment le haut niveau d'engagement des organisateurs, que je tiens à remercier chaleureusement. Elles soulignent aussi l'intérêt que présente un tel espace de réflexion et d'échanges pour les experts et décideurs que vous êtes.

Je me réjouis également que l'Allemagne soit à l'honneur cette année, et je tiens à saluer la présence parmi nous aujourd'hui de mon homologue et ami allemand, Thomas de MAIZIERE, qui est venu nous apporter son soutien dans cette période difficile où la France fait face à une crise sans précédent.

Le terrorisme frappe sans distinction de pays ni de continent : il est donc nécessaire que notre riposte soit commune, c'est-à-dire européenne et internationale.

Par ailleurs, nous sommes tous confrontés aux mêmes défis et à la même nécessité d'adapter nos réponses sécuritaires aux nouveaux usages numériques – je pense

notamment à la lutte contre la propagande et le recrutement terroristes sur Internet, qui est depuis des mois un sujet majeur de réflexion parmi les services européens de renseignement et de sécurité. Il a encore été l'un des grands enjeux dont mes homologues et moi-même avons discuté à l'occasion du G10 des ministres de l'Intérieur, que j'ai réuni en urgence place Beauvau le 11 janvier dernier. Je crois plus que jamais qu'en la matière, une meilleure coordination entre pays européens est un élément décisif de la réponse que nous devons apporter aux terroristes.

La participation du ministre allemand de l'Intérieur à l'inauguration du FIC 2015 illustre bien la dimension internationale de ce salon et des enjeux de cybersécurité. La présence des délégations étrangères de la FIEP (« France Italie Espagne Portugal »), association des gendarmeries euro-méditerranéennes, dont la France a pris récemment la présidence, est également une belle preuve de la dimension internationale que le FIC permet d'approfondir année après année.

Seul le prononcé fait foi

La révolution numérique concerne en effet toutes nos sociétés. Elle transforme aussi bien notre vie quotidienne que notre économie et notre modèle de production industrielle. Pour nos organisations, nos entreprises, nos collectivités territoriales ou encore nos administrations, elle représente un véritable levier de performance et un formidable accélérateur d'innovation, offrant des opportunités nouvelles de développement.

Néanmoins, le cyberespace est aussi aujourd'hui un champ sans frontières, où se développent des menaces pour notre société, de même qu'il est un outil susceptible d'être détourné à des fins malveillantes ou criminelles par des individus ou des organisations. Or, sur les territoires numériques comme ailleurs, la responsabilité de l'État est de protéger les citoyens avec détermination, d'anticiper les menaces, et de réprimer – lorsqu'ils surviennent – les actes délictueux.

Nous devons tout faire pour que le cyberespace soit avant tout un lieu où l'exercice des libertés fondamentales et la protection de la vie privée sont garantis.

Garantir la sécurité sur Internet n'est en effet rien d'autre qu'étendre aux territoires numériques – au cyberespace – la protection que nous devons à nos concitoyens, condition essentielle du respect des principes fondateurs de la République, et avant toute chose du respect de l'Etat de droit et des libertés individuelles, en toutes circonstances.

La sécurité dans les espaces numériques doit donc être assurée avec autant de détermination que dans nos villes et dans nos territoires. De même, le droit de vivre de son travail, c'est-à-dire d'innover et de développer une activité économique – ce qui de plus en plus implique une dimension numérique –, doit être garanti.

Une telle responsabilité engage la Nation tout entière. Nous l'assumons pleinement. Ainsi, face à la récente progression des phénomènes de radicalisation violente et d'endoctrinement terroriste sur Internet, aboutissant au départ pour la Syrie et l'Irak de plusieurs centaines de jeunes Français – et au départ, plus généralement, de nombreux jeunes Européens–, le Gouvernement a soumis

Seul le prononcé fait foi

au Parlement, qui les a adoptées dans la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, des mesures visant spécifiquement la diffusion de contenus illicites sur Internet – notamment des contenus de propagande terroriste et d'apologie du meurtre de masse ou de l'assassinats tels que ceux de notre compatriote Hervé GOURDEL ou de l'Américain Peter KASSIG.

Les attentats que nous avons dû affronter ont eux aussi largement démontré la centralité de ces enjeux de cybersécurité, et par là même l'absolue nécessité qu'il y a aujourd'hui à renforcer notre dispositif de lutte contre les cybermenaces. J'y reviendrai. Comme vous le savez, à la demande du Premier Ministre, nous sommes actuellement en train de finaliser de nouvelles propositions en la matière.

*

Ministère de l'Etat, ministère de la sécurité, de la prévention et de la gestion des crises, le ministère de

Seul le prononcé fait foi

l’Intérieur est donc particulièrement concerné par les trois dimensions fondamentales de la cybersécurité.

La **cyberdéfense**, tout d’abord, vise à protéger les institutions et les intérêts nationaux, conformément aux objectifs définis par le Livre blanc de la défense et de la sécurité nationale. Le ministère de l’Intérieur y participe activement, aux côtés de l’Agence nationale de la Sécurité des systèmes d’information (ANSSI) et du ministère de la Défense notamment.

La **sécurité des systèmes d’information** est un deuxième enjeu, tout aussi important. Il concerne non seulement les systèmes du ministère de l’Intérieur, mais aussi ceux de l’ensemble des acteurs économiques sur le territoire et des particuliers.

Enfin, la **lutte contre la cybercriminalité** mobilise aujourd’hui près de 600 enquêteurs spécialisés de la gendarmerie et de la police nationales.

C'est la raison pour laquelle j'ai nommé en décembre dernier un préfet spécifiquement chargé de la lutte contre

toutes les cybermenaces, le « préfet cyber », Jean-Yves LATOURNERIE. Directement rattaché à mon cabinet, et en lien permanent avec l'ensemble des directions générales et des directions du ministère qui sont concernées par les enjeux de cybersécurité, ainsi qu'avec les acteurs interministériels compétents, il a pour missions :

- de piloter la montée en puissance du dispositif ministériel, et de proposer le cas échéant des mesures d'organisation adaptées aux enjeux des cybermenaces ;
- de fédérer l'ensemble des énergies et les initiatives des différents acteurs au sein du ministère de l'Intérieur, et de veiller à ce qu'elles s'inscrivent dans le cadre de la stratégie ministérielle de lutte contre les cybermenaces ;
- d'être le point d'entrée identifié pour les acteurs extérieurs au ministère, notamment dans le cadre des travaux, engagés par l'ANSSI, visant à l'actualisation de la stratégie nationale de cybersécurité ;

Seul le prononcé fait foi

- enfin, de veiller à la pleine insertion de la démarche stratégique du ministère dans le cadre de la nécessaire coopération européenne et internationale.

Pour accomplir ses missions, le préfet LATOURNERIE bénéficiera bien sûr du concours de l'ensemble des services du ministère de l'Intérieur.

*

Avant d'évoquer les principaux axes de la stratégie ministérielle, je souhaite vous apporter quelques éléments qui permettront de mieux définir l'état des cybermenaces, tel qu'on peur l'appréhender aujourd'hui. Parmi les tâches confiées au « préfet cyber », figure justement l'élaboration d'un premier rapport ministériel sur l'état de la menace à laquelle nous devons faire face.

Les premiers travaux réalisés en vue de la rédaction de ce rapport permettent d'ores et déjà de dégager trois grandes tendances.

Seul le prononcé fait foi

Les différentes menaces que je vais brièvement décrire dans un instant, interviennent dans le contexte d'une société en profonde mutation numérique. Si le développement exponentiel des nouvelles technologies, l'émergence des objets connectés et les facilités offertes par le e-commerce sont de véritables progrès technologiques et sociaux, ils apportent aussi avec eux leur lot de difficultés nouvelles.

Les données numériques structurent en effet toutes les parties et étapes de notre vie personnelle et professionnelle, qu'il s'agisse des démarches administratives, de notre santé, de notre économie ou encore de nos loisirs.

Or, l'utilisation et la gestion de ces données très précieuses exposent aussi parfois leurs propriétaires à des menaces ou des vulnérabilités auxquelles nous nous devons d'apporter des réponses.

La première de ces menaces est le cyberterrorisme, qui consiste à commettre une action destructrice par le vecteur numérique. Comme je vous le disais, les groupes

terroristes qui nous ciblent sont extrêmement actifs sur les réseaux sociaux tels Facebook, Twitter et Youtube, tout en maintenant des canaux de transmissions plus traditionnels comme les forums djihadistes.

Même si les sociétés gestionnaires de ces médias sociaux sont aujourd'hui beaucoup plus soucieuses des contenus postés, l'utilisation d'Internet par les groupes ou organisations terroristes s'est encore amplifiée en 2014. Il apparaît nettement que les groupes islamistes radicaux les plus structurés (notamment Al-Qaida et DAESH) voient en Internet une tribune et un excellent vecteur de recrutement.

A cet égard, entre 2013 et 2014, le nombre de signalements parvenus au ministère de l'Intérieur par le biais de la plateforme PHAROS, créée à cet effet au sein de la Direction centrale de la Police judiciaire, a été multiplié par trois. Le fait que la grande majorité de ces signalements concerne des contenus détectés sur des réseaux américains, ne diminue en rien l'impact de ces actes de propagande sur nos ressortissants ou sur les

Seul le prononcé fait foi

étrangers résidant habituellement dans notre pays.

Les attentats auxquels nous avons dû faire face il y a une dizaine de jours, nous ont eux aussi démontré, si besoin était, que toute crise majeure – notamment terroriste – comporte désormais une forte dimension de cyber-sécurité. Ils ont ainsi confirmé la nécessité pour le ministère de l'Intérieur de se préparer à affronter les nouvelles menaces numériques en se dotant des outils et des ressources appropriés. Les réseaux sociaux servant de vecteur de communication aux terroristes, les supports numériques découverts ont été et sont encore exploités et analysés – entre autres par la sous-direction de la police judiciaire à la lutte contre la cybercriminalité – dans les délais très brefs imposés par la gravité et l'urgence de la situation.

Il a fallu ensuite faire face aux cyber-attaques malveillantes, prenant en la circonstance l'aspect d'un phénomène de masse inédit, modifiant les pages d'accueil ou exploitant les fragilités de milliers de sites institutionnels et privés. Plus de 1 300 attaques ont en

Seul le prononcé fait foi

effet été revendiquées par des équipes de hackers se revendiquant d'organisations islamistes ou saisissant l'opportunité de démontrer leur capacité malfaisante. Nous avons donc dû organiser très rapidement une réponse judiciaire commune que la sous-direction à la lutte contre la cybercriminalité a pilotée. Le réseau des investigateurs spécialisés en cybercriminalité de la police et de la gendarmerie nationales a également été mobilisé.

La plateforme PHAROS, elle-même mise à mal, a, durant la crise, traité en quelques jours plus de 25 000 signalements de contenus illicites sur Internet ; depuis les attentats, elle continue de veiller toujours aussi activement, grâce à la détermination sans faille des opérateurs policiers et gendarmes.

Enfin, une veille sur les réseaux sociaux a également été mise en place, exploitant, dans un tel contexte de crise, les contacts privilégiés noués avec les sociétés de service de l'Internet, plus particulièrement avec Twitter, Facebook, Google et Dailymotion. Un traitement particulier et en urgence a ainsi pu être accordé aux demandes de retrait des vidéos mises en ligne liées aux

Seul le prononcé fait foi

attaques terroristes. De manière complémentaire, les demandes de gel des données techniques liées aux demandes de retrait des vidéos ont été traitées 24H sur 24H pour le compte de l'ensemble des services de la police et de la gendarmerie nationale.

Le cyberterrorisme est une menace majeure, dont il convient de préserver nos compatriotes, nos institutions et les intérêts nationaux, comme le préconise le Livre blanc de la défense et de la sécurité nationale. Comme je vous le disais, le ministère de l'Intérieur travaille en étroite coopération avec l'ANSSI et le ministère de la Défense, pour mettre en œuvre notre stratégie de cyberdéfense.

La loi du 13 novembre 2014 a d'ores et déjà permis de renforcer nos moyens de lutte contre le cyberterrorisme.

L'un de ses principaux objectifs est en effet de lutter plus efficacement contre la propagande djihadiste, l'apologie et la provocation du terrorisme en ligne. Pour ce faire, nous avons prévu des dispositions permettant, sous le contrôle d'une personnalité qualifiée et le cas échéant du

Seul le prononcé fait foi

juge administratif, le blocage et le déréférencement des sites Internet qui mettent en ligne ce type de contenu. Le décret d'application relatif au blocage des sites sera publié dans les prochains jours, après les dernières consultations ; celui relatif au déréférencement suivra rapidement.

La loi comporte également des dispositions moins connues du grand public, mais tout aussi importantes dans la lutte contre la cybercriminalité : l'extension des cyberpatrouilles à l'ensemble des infractions relevant du champ de la criminalité organisée, l'introduction du délit de vol de données informatiques, l'aggravation des peines en matière d'atteinte en bande organisée aux systèmes de traitement automatisées de données de l'Etat et l'application de certaines techniques spéciales d'enquête, la facilitation des perquisitions informatiques et du déchiffrement des données cryptées.

Seul le prononcé fait foi

Sans doute notre dispositif législatif doit-il encore être amélioré – et nous allons bientôt faire de nouvelles propositions pour gagner en efficacité dans notre lutte contre le cyberterrorisme –, mais les enquêteurs sont d'ores et déjà mieux armés pour affronter les défis d'aujourd'hui et ceux de demain.

Le deuxième type de menace relève des cyberattaques contre les entreprises, qu'il s'agisse de cyberespionnage industriel ou de cyberescroquerie à grande échelle.

En effet, des attaques de plus en plus sophistiquées touchent principalement les entreprises et visent à leur voler des données stratégiques, parfois en très grande quantité comme certains exemples étrangers ou français l'ont montré ces dernières semaines, ou bien à leur soutirer des sommes importantes d'argent – plusieurs entreprises, parfois des multinationales, ont ainsi été récemment victimes d'escroqueries au faux ordre de virement international (FOVI).

Nous devons donc tout faire pour protéger nos entreprises de telles attaques. Les liens numériques qui unissent les fournisseurs, les vendeurs et les clients sont en effet désormais incontournables, et ne sont plus entravés par les frontières territoriales et politiques. Le patrimoine informationnel des entreprises revêt par ailleurs une importance capitale pour le développement de notre économie et la préservation de nos emplois. Ce patrimoine informationnel englobe très largement les données relatives aux projets liés à la recherche, l'innovation et le développement, les fichiers des clients ou des employés qui permettent de développer ou de préserver une activité économique et plus largement toutes données collectées, stockées et utilisées pour garantir le bon fonctionnement d'une entreprise. Stockées localement ou de manière délocalisée dans le « *cloud* », ces données sont essentielles pour le développement ou la survie de nos entreprises. Tout comme les locaux physiques, ces données peuvent faire l'objet d'attaque, de vols, de falsification ou de tous autres faits délictueux.

Enfin, le troisième type de menace dont nous devons tenir compte vise les particuliers, particulièrement vulnérables aux escroqueries en tous genres, qui s'accompagnent parfois de chantage sous forme numérique.

Ainsi, les escroqueries représentent actuellement 80% des plaintes cyber traitées par les services de police et de gendarmerie. En 2013, l'usage frauduleux de cartes bancaires dans les transactions sur Internet s'élevait à 155 millions d'euros. Les paiements à distance ne représentent que 11% de la valeur des transactions nationales par carte bancaire, mais comptent pour 65% du montant de la fraude.

Quant aux différentes formes de chantage sur Internet, on observe malheureusement le développement de plusieurs pratiques telles que le chantage suite à des vols massifs de données internes ou de clients d'entreprise, le chantage à la webcam (*sextorsion*), ou encore le chantage via l'utilisation de « rançongiciels ».

Là aussi, nous devons tout faire pour protéger nos concitoyens de telles menaces, qui violent par ailleurs leur intimité, ou ciblent leurs activités professionnelles.

*

Pour affronter ces défis, nous allons lancer **un grand plan d'action** qui renforcera l'efficacité des services du ministère de l'Intérieur en ce qui concerne la lutte contre les cybermenaces, quelles qu'elles soient.

Je l'ai dit au début de mon propos, la responsabilité de l'Etat, sur les territoires numériques comme ailleurs, est de protéger les citoyens, d'anticiper les menaces, de prévenir et de réprimer les actes malveillants et criminels. Depuis plus de 20 ans déjà, le ministère de l'Intérieur a intégré les défis nouveaux posés par la cybercriminalité. Mais aujourd'hui, l'ampleur et la variété du phénomène nous obligent à monter en puissance, à adapter notre dispositif de cybersécurité. Nous devons en effet mobiliser des compétences nouvelles, développer des moyens technologiques spécifiques, proposer des actions

Seul le prononcé fait foi

de protection et de prévention inédites à l'égard des systèmes et des publics particulièrement ciblés.

Surtout, à l'heure de la transformation numérique de la société, la lutte contre les cybermenaces ne peut plus être réservée à quelques experts : elle doit faire l'objet d'une organisation dédiée qui rendra possible l'amélioration et l'adaptation globales des services du ministère. C'est tout le sens du plan d'action élaboré par l'ensemble des directions du ministère, et dont la mise en œuvre sera pilotée par le « préfet cyber ».

Ce plan s'organise autour de six axes stratégiques.

Le premier axe consiste à disposer en permanence d'une vision claire et actualisée des cybermenaces.

Outre la production annuelle d'un rapport sur l'état de la menace, il s'agit de construire un appareil statistique adapté, permettant de mesurer les faits constatés dans le domaine de la cybercriminalité, mais aussi de disposer d'autres indicateurs externes ou internes au ministère de l'Intérieur caractérisant l'évolution de la menace. Le

Seul le prononcé fait foi

service statistique ministériel en sera le maître d’œuvre.

Le deuxième axe réside dans le renforcement de nos capacités d’analyse et de réponses opérationnelles.

Il s'agit pour ce faire de fédérer les énergies et de favoriser les échanges mutuels entre les divers services et forces de sécurité. La nomination du préfet en charge des cybermenaces contribue ainsi directement à cet objectif. Il s’agit aussi, chaque fois que possible, de mutualiser les efforts consentis au profit des acteurs opérationnels.

Nous disposons à l’échelon national d’un haut niveau d'expertise qui peut ainsi venir compléter et appuyer les dispositifs territoriaux de renseignement et des deux forces de sécurité police et gendarmerie dans le domaine judiciaire. Cet effort suppose une mobilisation générale de l'ensemble des services de renseignement, notamment de la direction générale de la sécurité intérieure (DGSI) et du service central du renseignement territorial (SCRT) dans le domaine cyber. Leur rôle d'anticipation sera également complété par une veille de l'internet, en

Seul le prononcé fait foi

particulier des réseaux sociaux.

Au sein de la Direction Centrale de la Police Judiciaire (DCPJ) a été créée en avril dernier la Sous-Direction de Lutte contre la cybercriminalité (SDLC). Elle réunit en son sein l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), qui comprend des policiers et des gendarmes, ainsi qu’une division de l’anticipation et de l’analyse. J’ai pu constater personnellement le rôle essentiel qui est le sien en cas de crise, et la réactivité, le savoir-faire et l’engagement de ses personnels.

Au sein de la Gendarmerie nationale, la Division de la Lutte Contre la Cybercriminalité (DLCC), transformée en Centre de Lutte Contre les Criminalités Numériques (C3N) sera rattaché au pôle judiciaire chargé de piloter la communauté des 1800 enquêteurs et correspondants « Technologies numériques de la gendarmerie ». Ce centre développera également ses capacités d'investigations d'initiative sur Internet.

Parallèlement, au sein des sections de recherches de la

Seul le prononcé fait foi

gendarmerie, des groupes cyber seront créés pour consolider les capacités d'investigations de haut niveau, y compris au plan territorial, et poursuivre les responsables de trafics de haut niveau, ou d’escroqueries en bande organisée.

L'adaptation des moyens consacrés au forces de sécurité, pour se moderniser et faire face aux cybermenaces tout en s'adaptant à la transformation numérique de la société, fait également l'objet de démarches mutualisées et communes aux deux forces . Ainsi l’organisation, sous le pilotage du préfet chargé de la lutte contre les cybermenaces, d’une veille juridique cyber à disposition de l’ensemble des services du Ministère, procède de cette démarche. Il en va de même en matière de formation à la lutte contre les cybermenaces pour l’ensemble des policiers et gendarmes, ou de la définition d’un schéma de mutualisation des formations des enquêteurs et investigateurs spécialisés dans ce domaine, qui associeront DGGN, DGPN et Préfecture de Police.

Plus largement, la lutte contre les cybermenaces s’inscrit

Seul le prononcé fait foi

dans le plan ministériel de modernisation, qui implique l'ensemble des services du ministère et permettra de consacrer sur le triennal 2015-2017 un budget total de 108 millions d'euros pour doter à court terme les forces de sécurité intérieure de moyens modernes et d'augmenter leurs capacités d'action, leur mobilité et leur sécurité. Ce plan vise à offrir dans le même temps de meilleurs services, notamment numériques, à la population pour une plus grande proximité des services. Il contribuera enfin directement à modernisation et la sécurisation des réseaux informatiques du ministère de l'Intérieur. Il s'agit pour nous de rester en mesure de faire face, y compris en situation de crise importante, aux exigences que nécessitent ses missions régaliennes

Le troisième axe porte sur la politique de sensibilisation et de prévention des publics.

En effet le ministère de l'Intérieur, du fait de sa présence sur l'ensemble des territoires, peut contribuer à améliorer significativement le niveau de vigilance des particuliers, des acteurs économiques et des collectivités territoriales.

Les réseaux territoriaux de la DGSI, de la DGGN et de la DGPN sont déjà particulièrement mobilisés par ces objectifs. La DGSI intervient directement auprès des opérateurs d'importance vitale et des entreprises les plus stratégiques. La gendarmerie concentre ses efforts sur les entreprises PME-PMI et a intégré les nouvelles menaces cyber dans ses actions de sensibilisation. Ces actions devront être encore amplifiées.

La prévention auprès des jeunes publics constitue également une priorité pour le ministère. Après les expérimentations conduites par la gendarmerie, l'ensemble des forces de la police, de la préfecture de police et de la gendarmerie s'engagent désormais dans l'opération "Permis Internet" auprès des élèves de CM2. Des initiatives particulièrement intéressantes ont été prises dans cette région, par la brigade de prévention de la délinquance juvénile du groupement de gendarmerie du Pas-de-Calais qui organise aujourd’hui même une opération à destination de sourds et malentendants ; un gendarme a ainsi été spécialement formé à la langue des signes.

Seul le prononcé fait foi

Le quatrième axe concerne la recherche et développement

Il est essentiel pour nous de disposer d'un tissu industriel solide, qui soit à même de proposer des solutions de cybersécurité éprouvées et qui préservent la souveraineté nationale. C'est pourquoi j'ai souhaité rencontrer dans quelques instants des représentants des entreprises françaises de cybersécurité. Je les rencontrerai accompagné de Jean-Yves Latournerie et de Thierry Delville, délégué ministériel aux industries de sécurité. Ma volonté est faire en sorte que l'Etat et les entreprises nouent une relation durable et solide, permettant à chacun de contribuer à l'amélioration du niveau de cybersécurité de la France. Le ministère de l'Intérieur devra donc jouer pleinement son rôle dans l'affirmation d'une politique industrielle de cybersécurité. Dans le prolongement des actions engagées par l'ANSSI au titre du plan 33 de la « Nouvelle France Industrielle » et dans le cadre des travaux menés au sein du comité de filière des industries de sécurité, le ministère de l'intérieur veillera à mobiliser toutes les énergies en faveur de l'émergence d'une offre

française, mais aussi européenne, de cybersécurité.

Dans le domaine de la formation, le partenariat noué entre la gendarmerie nationale et l'Université Technologie de Troyes pour la formation des « Enquêteurs technologies Numériques » illustre la qualité de ces échanges avec le monde de la recherche et de l'industrie. C'est pourquoi j'ai tenu à remettre leurs diplômes aux lauréats de la dernière promotion en compagnie du directeur de l'université M. Pierre Koch.

Le cinquième axe vise à renforcer encore le niveau de sécurité des systèmes d'information du ministère.

Dans ce domaine, le Ministère de l'Intérieur se doit évidemment d'être exemplaire. C'est pourquoi il nous faut à la fois actualiser régulièrement la liste des éléments essentiels de notre patrimoine opérationnel et conduire les audits de sécurité appropriés. Nous devons veiller à sensibiliser l'ensemble des personnels aux enjeux de la sécurité des systèmes d'information. Et nous devons bien entendu mettre à leur disposition des outils et systèmes qualifiés protégés, en particulier pour les usages mobiles.

Seul le prononcé fait foi

Je souhaite également que l’offre de services du Centre national de gestion de la sécurité des systèmes d’information soit actualisée. Il s’agit, là encore, de veiller à l’utilisation optimale des moyens importants que ce ministère consacre aux fonctions de veille, d’alerte et de réaction face aux incidents de sécurité informatique et de cyberattaques.

Le sixième axe consiste enfin à promouvoir l'action internationale du ministère dans le domaine de la lutte contre les cybermenaces

Face à des cybermenaces qui se jouent des frontières, la coopération avec nos partenaires étrangers revêt un caractère fondamental. La Direction de la Coopération Internationale (DCI) est résolument impliquée dans cette ambition et son réseau international s’est mobilisé afin d’appuyer au quotidien l’activité des acteurs opérationnels, (SDLC, C3N, PP.) hors de notre territoire.

La coopération judiciaire doit bénéficier de législations internationales adaptées à des besoins opérationnels qui restent souvent conditionnés par l'urgence. C'est pourquoi j'ai demandé au préfet chargé de la lutte contre les cybermenaces de s'assurer de la cohérence des travaux d'élaboration de la doctrine internationale en la matière.

A cet effet l'ensemble des directions travaille à améliorer le dispositif au niveau de l'Union européenne, du Conseil de l'Europe et dans d'autres enceintes de négociation. En effet, la sécurité de l'espace cyber demeure une sécurité collective. De ce fait, elle repose sur l'échange de compétences entre les professionnels des forces de l'ordre. En 2014, près de 300 partenaires étrangers ont bénéficié de ce partage de compétence de la part de nos services. Ce sont ces partenaires qui, ayant noué de solides relations de confiance mutuelle, contribueront demain aux succès des enquêtes internationales.

Dans le même esprit, j'invite également nos partenaires

Seul le prononcé fait foi

étrangers à développer leurs contacts avec les 280 policiers et gendarmes des 84 représentations du ministère de l’Intérieur qui se trouvent au sein de nos ambassades à l’étranger. Je les remercie aussi pour le soutien qu’ils pourront nous apporter dans le cadre des négociations visant à établir des cadres juridiques qui répondent mieux aux attentes des enquêteurs.

*

Enfin, je voudrais souligner que la lutte contre les cybermenaces ne peut se concevoir au sein du seul ministère de l'Intérieur. Notre approche doit être globale et transversale et elle a donc vocation à s'inscrire plus largement dans un contexte interministériel. De nombreux autres départements sont mobilisés par ce sujet, à commencer par celui de la Défense et par celui de l’Economie et des Finances. C’est pourquoi je me félicite de la venue demain ici même, à l’occasion de la clôture de ce Forum, de mes collègues Axelle Lemaire et Jean-Yves Le Drian.

C'est dans le même esprit que je vous souhaite donc de

Seul le prononcé fait foi

profiter pleinement de cette occasion exceptionnelle que constitue ce Forum pour dialoguer et échanger avec de nombreux experts et décideurs, issus des entreprises, des administrations ou de l'Université, venus de France ou de pays étrangers, afin de confronter nos visions respectives de la transformation numérique qui est à l'œuvre au sein de nos sociétés.

Je vous donne enfin d'ores et déjà rendez-vous pour la prochaine édition de Forum en 2016. Vous pourrez compter naturellement sur l'engagement du ministère de l'intérieur, et au sein de celui-ci sur celui de la gendarmerie nationale dont je tiens à saluer la remarquable et persévérante contribution à cette initiative.

Je vous remercie.

Seul le prononcé fait foi