Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

**Allocution de M. Laurent NUNEZ, secrétaire d'État auprès du ministre de l'Intérieur**

**11ème Forum International de la Cybersécurité**

*Lille*

*Mardi 22 janvier 2019*

---

*Seul le prononcé fait foi*

**Monsieur le Commissaire européen, (Sir Julian KING),**
**Monsieur le Préfet de la Région, (Michel LALANDE),**
**Monsieur le vice-président de la Région Hauts de France (Nicolas LEBAS), représentant M. Président de la Région, (Xavier BERTRAND)**
**Mesdames et Messieurs les parlementaires,**
**Mesdames et Messieurs les élus,**
**Monsieur le Préfet, coordonnateur national pour le renseignement et la lutte contre le terrorisme,**
**Monsieur le directeur général de la gendarmerie nationale, (Général d'armée Richard LIZUREY),**
**Monsieur le directeur général de la police nationale, (Préfet Eric MORVAN),**
**Monsieur le président du conseil de surveillance de CEIS, (Olivier DARRASON)**
**Mesdames Messieurs les industriels, entrepreneurs, chercheurs, start-upper, fonctionnaires, militaires,… tous acteurs de la cybersécurité,**
**Mesdames Messieurs,**

C'est un plaisir pour moi d'ouvrir pour la première fois, en tant que membre du gouvernement, ce Forum international de la cyber sécurité, cette 11ème édition du FIC.

LILLE est à l'intersection de nombreuses voies européennes, physiques et numériques. Ce matin plus encore avec ce rendez-vous devenu incontournable pour les acteurs mondiaux de la cybersécurité.

**Je veux remercier tout d'abord les organisateurs** pour ce forum annuel préparé avec grande efficacité :

- le directeur général de la gendarmerie nationale et ses équipes, en particulier le général Watin-Augouard, toujours fidèle au poste ;
- la Compagnie européenne d'intelligence stratégique, CEIS, et son président Guillaume Tissier :
- et le président de cette dynamique région Hauts-de-France qui nous accueille pour ces deux jours.

Je veux saluer également l'engagement des partenaires, près de 110, sans lesquels ce forum ne pourrait se tenir. Je remarque aussi que parmi eux nous retrouvons tous les leaders mondiaux du secteur.

Je remercie bien sûr l'ensemble des services participants du ministère de l'intérieur : DICOM, gendarmerie, police, services spécialisés qui œuvrent dans ce domaine sensible.

Votre présence démontre que la sécurité numérique est bien au cœur des préoccupations des décideurs politiques et économiques.

**Enjeux et lien avec le thème du FIC**

Si nous sommes rassemblés ce matin, c'est que nous partageons la conviction que la cybersécurité constitue un enjeu majeur pour nos sociétés.

Cet enjeu n'est d'ailleurs pas nouveau. Je suis certain que dès le 1er FIC en 2007, nous parlions déjà des **escroqueries en ligne**. Elles se sont malheureusement bien améliorées depuis, et les mails en mauvais français facilement détectables sont plus rares. En revanche, les techniques de phishing sont plus sophistiquées, elles permettent aussi de toucher davantage de personnes, augmentant ainsi l'espérance de gain. Elles restent d'actualité pour nous tous.

De même, pour les **attaques de système d'information**. Le premier FIC fêtait quasiment les 10 ans de la loi Godfrain qui les réprimait. Et pour autant, cet enjeu est toujours bien présent et se renouvelle en raison d'une plus grande connectivité des systèmes, de la multiplication des terminaux de tous types, d'une limite usage privé / usage professionnel plus ténue, du développement des services en ligne. Cette interdépendance est une force mais aussi une vulnérabilité.

D'autres défis sont plus récents.

2018 s'est ainsi achevée comme 2017 avec un haut niveau de cyberattaques, entrainant des **fuites importantes de données** professionnelles et personnelles. Ces fuites ont concerné une personne sur 12, oui je dis bien une personne sur 12, ce qui a fait de 2018 une année terrible.

La semaine dernière, nous apprenions l'existence d'une base de données comprenant jusqu'à 772 millions d'adresses mail piratés et plus de 20 millions de passeport. Cela interroge chacun d'entre nous sur sa propre sécurité et la protection de ses données.

La mise en œuvre du RGPD (règlement général sur la protection des données) et de la directive européenne NIS (Security of Network and Information System) devraient aider tous acteurs à mieux se protéger. On désigne des secteurs et des opérateurs de services essentiels qui doivent renforcer leur sécurité et alerter l'ANSSI, laquelle doit veiller à diffuser ces éléments auprès des services spécialisés de répression comme de renseignement.

Le développement du **darkweb** constitue également un défi, en ce qu'il permet le développement de **marchés criminels en ligne**. Ces nouveaux espaces proposent à la vente des stupéfiants, des armes, des médicaments, des codes de cartes bancaires, mais aussi des outils informatiques malveillants. Réservés aux initiés dans un premier temps, ils sont désormais plus facilement accessibles pour une génération « digital native ». Ils permettent en outre une navigation anonyme.

Mais, ce ne peut rester un espace sans droit. Les enquêtes doivent pouvoir s'y déployer et je salue à cet égard le recours grandissant aux enquêtes sous pseudonyme par la police et la gendarmerie. Des enquêtes judiciaires récentes ont montré l'intérêt de ces investigations.

Aux confins de la problématique cyber et dans son articulation avec les réseaux sociaux et son rôle de véhicule d'information, le cyber devient également une arme de **manipulation des opinions**. Je pense à la diffusion virale de fake news. La proximité d'échéances électorales est à ce titre un sujet de préoccupation.

Pour remédier à cette propagation, le Gouvernement a fait adopter **une nouvelle législation le 20 novembre 2018 avec une loi ordinaire sur la manipulation de l'information et une loi organique applicable à l'élection présidentielle.** C'est une réponse à la fois mesurée mais ferme par rapport à ceux qui voudraient fragiliser notre société et intervenir dans notre système électoral.

Une autre forme de défi nouveau **: l'internet des objets et la 5G**. Prenons l'exemple de la voiture connectée – voiture autonome. C'est, du point de vue de la cybersécurité, un challenge en termes de sécurité de la conduite, de protection des données personnelles, de risque de piratage des nombreux objets qui s'y connectent à commencer par nos propres smartphones. La multiplication de ces objets dans notre vie quotidienne, dans notre vie professionnelle exige une vraie sécurité. Par construction, mais encore plus à cause de failles de sécurité.

La sécurité doit être intégrée dès la conception des produits et des applications, c'est la **Security by design** comme s'est imposée la **Privacy by design**. Tel est le **double thème que vous avez choisi pour ce forum international**, qui reflète ainsi deux impératifs forts du ministère de l'Intérieur, garantir la sécurité et protéger les libertés.

J'ai en effet deux convictions :

- Exercer ses libertés impose un espace sûr, le ministère de l'intérieur a la responsabilité de la protection de ces libertés, il est en le garant ;
- Les dangers des territoires numériques impactent massivement la vie réelle, l'espace physique. La crise cyber, le cybercrime ont des conséquences dans la vie de nos concitoyens, de nos entreprises (perte d'argent, chantage, indisponibilité de services publics,…). La crise cyber ou le cybercrime viennent troubler l'ordre public. Nous sommes là au cœur de la mission du ministère de l'intérieur, la gestion de crise, dans une logique de continuum espace numérique-territoire physique, qu'il nous faut prendre en compte.

C'est bien l'enjeu de votre Forum, comment concilier ce formidable potentiel de liberté, d'échanges, de progrès, avec des exigences absolues, totales de sécurité. Il faut, nous devons, parvenir à cet équilibre. Nos concitoyens attendent de nous la réussite de ce challenge.

Aussi, je me félicite que le ministère de l'intérieur soit associé à ce forum et que nombre de ses membres aient été invités à s'exprimer dans de nombreux ateliers tout au long de ces deux jours.

Les réalisations 2018

Les enjeux sont multiples et évolutifs, je viens de le rappeler. Le ministère de l'Intérieur doit ainsi en permanence s'adapter et anticiper les menaces.

Il en a pris conscience et nous avons demandé un renforcement de ses capacités car les technologies numériques sont aussi une opportunité pour moderniser son action et améliorer son efficience.

L'intelligence artificielle, l'Internet des objets, nous invitent à réfléchir le futur, pas uniquement de manière politique ou technique. J'ai appris d'ailleurs qu'une session de travail intitulée « Philoso-FIC » (avec un très joli jeu de mot alliant « philosophie » et « FIC ») va aborder ce thème. Je demanderai à mes services de m'en faire un compte-rendu précis. Car mon expérience m'a appris que la réflexion précède l'action, même à la tête du ministère de l'urgence.

Plus concrètement, beaucoup de choses ont été conduites ces dernières années. Je peux affirmer que le ministère de l'intérieur est dans une dynamique forte en matière de cyber.

Nos **dispositifs de lutte contre les arnaques et les escroqueries en ligne, tout d'abord,** évoluent. Au-delà de la traditionnelle plainte au commissariat de police ou à la brigade de gendarmerie -qui reste possible-, nous proposons désormais aux victimes d'usage frauduleux d'une carte bancaire une plate-forme de signalement : la plateforme **PERCEVAL**, opérée par la gendarmerie nationale.

Facile d'accès, rapide, elle simplifie les démarches des victimes. Parce qu'elle permet de recueillir un grand nombre de signalements, elle apporte une vue plus complète des phénomènes de fraude et permet d'améliorer la détection des fraudes massives.

En 6 mois, elle a recueilli 69 000 signalements, pour un préjudice total de 33 M€. Autant de victimes qui ont pu faire valoir leurs droits.

Mais aussi, des rapprochements qui se sont traduit par l'ouverture de 55 enquêtes judiciaires et l'identification à ce stade d'une trentaine d'auteurs.

**Intervenir en amont** est également l'une de nos priorités.

- C'est pour cela que nous soutenons activement **ACYMA**, le « dispositif d'assistance aux victimes d'actes de cybermalveillances ». Ce GIP, dont le ministère est membre, a en 2018 orienté 28 000 victimes vers des solutions concrètes de remédiation en lien avec ses 1 600 prestataires référencés. Son premier kit de sensibilisation à destination des PME a quant à lui été téléchargé plus de 18 000 fois. C'est de bonne augure et j'aurais plaisir à me rendre chez ACYMA dans deux jours pour saluer ce travail essentiel de prévention et d'asssistance.
- De même, le ministère de l'Intérieur a mis en place avec le ministère de l'Education nationale **un permis Internet** sur les dangers à destination des scolaires. Depuis 2013, plus d'un million et demi d'enfants ont ainsi été sensibilisés.
- Je n'oublie pas les **entreprises** et l'action en particulier de la DGSI, service que j'ai eu l'honneur de diriger et dont je salue le directeur technique : devant les nombreux industriels qui sont ici présents, je tiens à rappeler une évidence. Vous faites tous partie à un degré plus ou moins marqué d'un écosystème pouvant être la cible d'acteurs cyber malveillants.
  Vous êtes tous des cibles pour des attaquants. Et vous êtes d'une manière ou d'une autre un maillon dans une chaîne de valeur. Il suffit d'un maillon faible pour que le service ne soit plus rendu, ou que des données soient volées. C'est ça la latéralisation des attaques, vous êtes ciblé pour servir de rebond !

C'est pourquoi je ne peux que vous inciter à vous rapprocher pour les plus sensibles d'entre vous, en particulier pour ce qui a trait au patrimoine scientifique et technique, et donc parfois aux intérêts fondamentaux de la Nation, de la DGSI pour bénéficier de conseil ou pour signaler toute éventuelle attaque. Si vous avez le moindre doute d'être pillé ou espionné, vous devez contacter la DGSI, elle bénéficie d'un maillage complet du territoire et vous trouverez toujours une personne proche de vous que vous pourrez contacter en toute discrétion. Vous savez combien la culture du secret est grande dans cette maison, vous pouvez travailler en confiance.

Plus classiquement, la **lutte contre la cybercriminalité** constitue une responsabilité essentielle du ministère. Le ministère peut s'appuyer à ce titre sur un maillage territorial décisif et des compétences incontestables : 80% des policiers et des gendarmes formés au cyber sont ainsi déployés dans les territoires. Ces réseaux se renforcent.

- Ainsi, la police nationale a créé un réseau de référents cyber zonaux à titre expérimental sur trois régions pilotes, Grand-Est, Bretagne et Nouvelle Aquitaine, pour sensibiliser le tissu économique local au risque cyber ainsi qu'à la délinquance financière par l'animation d'un réseau partenarial zonal et local entre les services de police judiciaire et le secteur privé. En effet, je le rappelle 63 % des cyberattaques ciblent des entreprises.
- Mais ces agents ce sont aussi des enquêteurs sur le volet répressif.
- Et ces enquêteurs cyber ont besoin d'être formés. Des efforts importants sont réalisés pour cela. J'ai ainsi remis, il y a quelques instants, les diplômes délivrés par l'université de Troyes à 6 enquêteurs NTECH (lire « N » « Tech ») de la gendarmerie nationale, issu de la dernière promotion. Formés à haut niveau, ils sont directement employables pour réaliser des enquêtes cyber ou des actes de criminalistique numérique. Je salue à cet égard l'action résolue du centre de lutte contre les criminalités numériques de la gendarmerie – le C3N – et du **réseau Cybergend** qui fédère à ce jour plus de 4500 enquêteurs numériques à travers tout le territoire, effectif que souhaitons doubler d'ici 2022.

**Sur la méthode**, nous évoluons également, en privilégiant les partenariats, à l'instar du **Centre de réponse à incident** créé au sein de la police judiciaire pour anticiper les menaces cyber et soutenir les actions judiciaires contre la cybercriminalité. Il est devenu un vecteur de coopération technique en matière de cybersécurité et a rejoint la communauté européenne des centres de réponse à incident animé par l'ANSSI (agence nationale de la sécurité des systèmes d'information). Il a noué des partenariats forts avec plusieurs acteurs du secteur privé français spécialisés notamment dans le conseil, les antivirus, l'analyse de données, ou la lutte contre le phishing.

Je ne peux oublier **la lutte contre le terrorisme**. Il faut rappeler que celui-ci continue de se propager sur internet. La France et ses partenaires allemands et britanniques ont joué un rôle décisif pour parvenir à une initiative législative européenne garante de l'efficacité à long terme dans la lutte contre les contenus terroristes en ligne. Publié le 12 septembre 2018, ce projet de règlement, en cours d'adoption, porte sur la prévention des contenus terroristes en ligne et permet leur retrait en moins d'une heure après le signalement. Certes beaucoup a été fait avec les plateformes mais trop ne jouent pas le jeu.

Ce texte européen n'épuise pas le débat sur la régulation d'Internet. La France souhaite aussi étendre l'obligation de retrait en cas de diffusion de contenus haineux, racistes ou antisémites en ligne. La lutte contre la haine en ligne doit être juridiquement encadrée et ne plus seulement reposer sur le volontarisme des plateformes. Cette question est également au cœur de l'initiative engagée avec Facebook par le gouvernement sur la haine en ligne, annoncée par le président de la République

à l'internet gouvernance forum, le 12 novembre 2018. Là encore, les opérateurs ont fait des efforts et je salue leur participation, mais on doit renforcer le caractère universel du retrait et améliorer encore les délais. La France souhaite comme ses partenaires européens que toutes les plateformes opèrent avec la même méthode et la même exigence. Je fais confiance aux opérateurs présents ici au FIC pour aller dans ce sens de la protection de nos concitoyens.

Si les contenus terroristes se distinguent des contenus haineux par le fait que la liberté d'expression peut être opposée à ces derniers, nous devons parvenir à obtenir les retraits les plus rapides de ces contenus porteurs de haine.

Je salue à cet égard tout l'intérêt de la plateforme PHAROS de la DCPJ qui accomplit un travail décisif en recueillant vos signalements et ceux de tous les intervenants, ce qui nous permet d'améliorer notre perception des phénomènes.

Enfin, la **coopération internationale** fonctionne. Je veux vous donner un exemple très concret qui va rassurer Monsieur le Commissaire européen.

Une société financière britannique a été victime en mai 2017 d'attaques informatiques, d'extraction de données et de tentative d'extorsion de fonds de 730.000 Livres par des hackers français se revendiquant du groupe Rex Mundi, localisés en France et en Thaïlande.

Grâce à la coopération d'EUROPOL avec les services de police et de gendarmerie, l'ensemble du groupe de pirates a été arrêté, depuis le concepteur du code jusqu'aux « petites mains », entre octobre 2017 et mai 2018. La coopération internationale permet de mieux défendre vos entreprises contre les tentatives d'escroquerie, même si votre vigilance reste votre meilleure protection.

Cette coopération fonctionne aussi en matière d'échanges d'informations et de renseignements, mais vous comprenez bien que je ne peux en dire plus ici.

## L'ambition du ministère et du gouvernement

**Ce large panorama vous dresse le bilan d'une activité 2018 très chargée du ministère** que j'ai l'honneur de diriger avec Christophe CASTANER avec lequel nous avons décidé de passer la vitesse supérieure.

**2019 sera une année décisive à plusieurs niveaux en matière de cyber :** le Gouvernement avec la filière industrielle de sécurité ; le ministère de l'Intérieur avec une feuille de route cyber.

Le Gouvernement a décidé en novembre dernier **d'intégrer la filière des industries de sécurité au sein du Conseil national de l'industrie**, afin de donner aux entreprises de ce secteur les moyens de réaliser ses ambitions à l'horizon 2025.

Cette transformation n'est pas anodine et ne vise pas seulement à soutenir la croissance des entreprises qui se situe en moyenne à 5,6% avec une pointe à plus de 12 % pour les acteurs du cyber. Le Gouvernement souhaite aussi que ce secteur puisse créer plus de 30.000 emplois qualifiés et multiplier ses exportations qui constituent déjà plus de 56 % de son chiffre d'affaires.

La confiance numérique compte deux des six grandes familles de la filière industrielle et représente avec ses produits, ses solutions et ses services 10,5 milliards d'euros de chiffre d'affaires sur un total

de 29,5 milliards. La France compte plus de 13 leaders mondiaux dans cette filière qui tire la croissance vers le haut et dont le dynamisme se diffuse sur l'ensemble du territoire par une multitude d'entreprise de taille intermédiaire, de PME-PMI et de start-up stratégiques qui ont d'ailleurs brillé au dernier CES de Las Vegas. Je sais que la Région Hauts-de-France y était bien représentée.

Un contrat de filière sera élaboré dans les prochains mois en collaboration entre l'Etat et les industriels eux-mêmes afin d'atteindre les objectifs fixés d'ici 2025. Les technologies clés comme l'intelligence artificielle, les objets connectés et le big data seront bien sûr au cœur de ce contrat de filière et contribueront à la sécurisation des territoires intelligents, à la sécurité des grands événements tels que les JO 2024 et à la souveraineté numérique. Des engagements réciproques favoriseront une action coordonnées et efficace de l'ensemble des acteurs publics et privés, donc vous, de la filière. Nous avons besoin d'un secteur cyber fort. Je le redis : ce sont aussi et surtout des enjeux de souveraineté qui se jouent.

Enfin, le ministère de l'Intérieur adoptera une **feuille de route du ministère dans le domaine cyber** qui a été rédigée par la délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC) avec l'ensemble de directions générales et services du ministère de l'Intérieur. Je voudrais saluer ce travail.

Cet exercice inédit a permis de réaliser un audit et de constater que plus de 8.600 personnels du ministère ont été formés dans ce domaine et qu'ils sont répartis sur l'ensemble du territoire national, seulement 20 % d'entre eux sont en administration centrale. C'est dire le maillage territorial tissé avec des compétences incontestables et décisives en cas de crise majeure.

Ce travail s'est appuyé sur l'état annuel de la menace cyber, qui est d'ailleurs consultable sur internet, également rédigé par la DMISC et tous les services du ministère. Il se veut à la fois un outil de prévention et de sensibilisation des entreprises, grandes ou petites, des collectivités territoriales, des services publics et des citoyens face à ces nouvelles menaces.

La validation de cette feuille de route est imminente car je veux fixer les axes qui vont engager le ministère de l'Intérieur pour les années à venir qui seront cruciales pour notre sécurité.

La gouvernance cyber du ministère sera renforcée. Le rôle pilote de la Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC) est confirmé. Un nouveau délégué sera nommé prochainement à la suite de Thierry Delville à qui je voudrais rendre hommage.

Nous recrutons grâce à une politique RH innovante et audacieuse 800 agents supplémentaires, consacrés à la lutte contre les cybermenaces au sein de l'ensemble des directions opérationnelles, et à la sécurité des systèmes d'information.

Le ministère de l'intérieur, c'est la sécurité, qu'elle soit numérique et physique. Nous l'assurerons et ferons face aux menaces qui évoluent en permanence. La traduction budgétaire est forte pour le MI, comme en témoigne l'augmentation de 20 M€ du budget de la DGSI en matière d'équipements techniques.

Bien sûr, j'aurais pu aborder d'autres questions. Je pense aux réflexions en cours au niveau interministériel sur l'identité numérique. Je pense, bien sûr, aux réflexions en cours sur la preuve numérique et sur la possibilité pour nos services de police judiciaire d'accéder aux données détenues hors de l'Union Européenne.

## Conclusion

Mesdames et messieurs,

Avec Christophe CASTANER, nous proposerons au président de la République, au Premier ministre, le débat d'une loi de programmation afin de fixer la vision à long terme de notre politique de sécurité intérieure, fondée sur le continuum de sécurité. La sécurité doit être efficace sans être contraignante et elle est sans cesse renouvelée par l'urgence des situations à traiter et des défis futurs à anticiper.

Le progrès génère autant sa partie lumineuse que sa partie sombre. Au travers de mes anciennes fonctions de DGSI, je connais tout particulièrement ce contexte. Il nous revient avec toutes les femmes et les hommes de ce ministère d'en combattre les effets négatifs et d'en valoriser les bénéfices au profit de nos concitoyens qui souhaitent être protégés tout en restant libres.

Ces valeurs fondamentales sont les nôtres. Il est dans notre mission de les protéger et de les défendre, et encore plus à l'ère du numérique. La sécurité est une course sans fin et comptez sur nous pour rester en tête.

Je sais aussi pouvoir compter sur vous tous.

Je vous remercie.

**Service de presse de M. Laurent NUNEZ, secrétaire d'État auprès du ministre de l'Intérieur**

**01 49 27 38 53 - sec1.pressecab@interieur.gouv.fr**