MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

Madame Florence Parly,

ministre des Armées

Signature de la convention avec le groupement d'intérêt public Action contre la Cybermalveillance

Paris, le 4 mars 2021

– Seul le prononcé fait foi –

Mesdames et messieurs les élus,
Monsieur le président,
Monsieur le directeur général,
Messieurs les officiers généraux,
Mesdames et messieurs,

Je remercie vivement le groupement d'intérêt public Action contre la cyber-malveillance pour son accueil aujourd'hui et pour la qualité des présentations qui ont été réalisées.

A l'aube du XIXème siècle, le lexicographe Pierre-Claude-Victor Boiste écrivait dans son dictionnaire universel, à propos de la malveillance, « elle ne dort que d'un œil, cherche toujours des idées pour troubler notre repos et nuire à nos intérêts. »

S'il existe bien un espace où la malveillance ne dort jamais, pas même d'un œil, un espace où chacun d'entre nous peut devenir la cible, le vecteur, voire même l'amplificateur de sa menace, c'est bien l'espace cyber.

Aujourd'hui, la menace numérique est tout sauf virtuelle. Les cyberattaques qui étaient encore invisibles aux yeux de nos concitoyens il y a quelques années, et même quelques mois, font désormais la « une » des journaux.

En seulement un an, entre 2020 et 2021, les attaques cyber ont été multipliées par quatre. Elles ne touchent plus seulement les grandes entreprises et les géants de la tech, elles s'immiscent dans notre vie quotidienne en ciblant des particuliers, des collectivités locales et même des hôpitaux, c'était le cas en 2019 avec l'hôpital militaire Sainte-Anne à Toulon, et ce fut aussi plus récemment celui de Dax, au cœur de la crise sanitaire, il y a seulement quelques semaines.

C’est dans ce contexte de multiplication et de sophistication des attaques que le Président de la République a fait, le 18 février, des annonces ambitieuses et nécessaires pour la stratégie nationale de cybersécurité.

Pour ce qui concerne le ministère des Armées, nous avons consacré 1,6 milliard d’euros à la cyberdéfense sur la période 2019-2025 grâce à notre Loi de Programmation Militaire, et nous avons élaboré une feuille de route rigoureuse en la matière en 2019, qui s’inscrit pleinement dans les ambitions de cette stratégie nationale de cybersécurité.

Le Commandement de la cyberdéfense créé en 2017, et aujourd’hui représenté, travaille étroitement avec l’Agence nationale de sécurité des systèmes d’information pour bâtir notre défense numérique. Nous avons l’objectif, qui n’est pas facile à atteindre car leurs compétences sont rares et recherchées, de recruter 1 000 cybercombattants d’ici 2025.

Une de nos priorités est de faire de notre pays un champion de la cyberdéfense. Dans ce domaine, le ministère des Armées a des missions et des enjeux qui lui sont propres : comme l’a souligné le Président de la République, l’arme cyber peut être employée par d’autres puissances étatiques, par des groupes terroristes ou, et c’est plus insidieux, par leurs soutiens. Sur le théâtre de l’opération Barkhane au Sahel, nous avons récemment constaté une augmentation des attaques.

Mais qu’il s’agisse d’une cyberattaque en opération extérieure ou au sein d’un hôpital, le résultat est le même : une paralysie temporaire des systèmes d’information condamne le militaire ou le professionnel de santé à agir dans une situation dégradée, sans avoir la pleine possession des moyens d’imagerie, de communication et d’accès aux données qu’il a l’habitude de mobiliser pour accomplir pleinement sa mission.

Les menaces cyber touchent aujourd'hui tous les segments de la vie quotidienne, elles ne connaissent aucune frontière, se déploient et évoluent avec une rapidité et une vélocité accrues. Pour mieux les comprendre et les contrer, il est indispensable de construire un cercle de confiance avec tous ceux qui œuvrent à protéger un monde numérique contre la cyber malveillance.

Nous le savons, les hackers cherchent à exploiter toutes nos vulnérabilités, en ciblant nos partenaires moins aguerris dans l'espace cyber, en ouvrant toutes les brèches qu'ils détectent. C'est pourquoi le ministère des Armées porte l'ambition de renforcer sa chaine de cyberdéfense de bout en bout, de l'administration centrale à la PME sous-traitante d'un grand groupe de défense, comme cela vient d'être illustré par Naval Group.

C'est dans cet esprit que nous avons signé en 2019 une convention cyber avec les grands maîtres d'œuvre industriel de défense pour mieux prendre en compte les enjeux cyber dans toutes leurs dimensions et créer ce cercle de confiance qui nous permettra de faire face aux dangers du cyber.

Car l'expérience des dernières cyberattaques nous a démontré que la cybersécurité doit se construire de façon collective, par le partage d'informations et et le partage de bonnes pratiques entre les acteurs privés et les acteurs publics.

Et c'est là un des enjeux du partenariat entre le GIP Acyma et le ministère des Armées et dont nous allons signer la convention dans quelques minutes. Nous sommes fiers de ce nouveau partenariat qui s'inscrit pleinement dans le **deuxième axe de la stratégie présentée par le Président de la République qui consiste à renforcer les liens et les synergies entre les acteurs de la filière pour fédérer l'écosystème de la cybersécurité.**

Le GIP Acyma est aujourd'hui un maillon essentiel d'assistance, de prévention et de lutte contre la cybercriminalité. Vous avez acquis une expertise unique et reconnue pour accompagner les victimes d'actes de cyber-malveillance et aussi pour sensibiliser les citoyens aux cyber-menaces. En alliant les compétences et les ressources des membres issus du secteur privé avec celles du secteur public, vous êtes devenus des acteurs incontournables de la sécurité numérique : **s'associer avec vous, c'est donc rejoindre une communauté de compétences au service d'une mission d'intérêt général.**

Ce nouveau partenariat permettra de nourrir la connaissance des menaces et des attaques avérées au sein de la sphère défense. Je sais que nous avons beaucoup à apprendre de vous et que cette association fructueuse conduira à augmenter le niveau général d'expertise du ministère des Armées en retour dans le domaine des cyber activités malveillantes.

Concrètement, le **ministère des Armées va mettre à votre disposition un officier de la direction du renseignement et de la sécurité de défense, la DRSD, à temps plein**.

Vous pourrez donc vous appuyer sur les compétences de la DRSD, service de renseignement disposant de compétences sur une très large part du spectre de la cyber sécurité, de l'anticipation à la réponse à incident en passant par la protection et la détection. Sa connaissance de cas concrets d'attaques informatiques et de compromission du secret et son étroite coopération avec les autres acteurs clefs de la cyberdéfense au sein du ministère des armées ainsi qu'avec l'ANSSI, sont à mes yeux de véritables atouts pour les actions de sensibilisation effectuées auprès des entreprises de notre base industrielle et technologique de défense.

Je suis convaincue que la DRSD a également beaucoup à vous apporter. Chaque jour malheureusement, elle est le témoin de comportements malveillants nouveaux et de plus en plus sophistiqués. A titre d'exemple, car ils parlent plus que les théories, la DRSD a observé, au second semestre 2020, une large mobilisation d'individus menant des actions cyber offensives et propagandistes à caractère islamiste. Ces actions ont conduit à une vague de défigurations de sites web d'entités ou de personnes physiques françaises liées à la sphère Défense. La DRSD a donc fourni son appui pour stopper ces attaques et identifier, quand cela était possible, les attaquants.

Dans le domaine de l'espionnage industriel, la DRSD a aussi identifié de nombreux cas d'ingénierie sociale : c'est-à-dire des techniques de manipulation psychologique qui sont utilisées par les cybercriminels pour inciter les gens à partager des informations confidentielles. Les entreprises visées par ces opérations ont été sensibilisées et conseillées par le ministère.
Enfin, **la DRSD dispose d'un maillage territorial historique indispensable à la coopération de proximité quotidienne** avec les acteurs de la sphère Défense. **Cette présence dans les régions aux côtés des ExpertCyber labellisés par Acyma,** qui reconnait l'expertise numérique des professionnels de service informatique, est tout à fait cohérente avec l'orientation stratégique présentée par le Président de la République : il s'agit de **renforcer les synergies dans les régions entre petits et grands acteurs de la filière cyber et entre industriels et recherche.**

Une complémentarité sera aussi recherchée avec le dispositif Diag Cyber, dont je suis très fière et dont je regrette qu'il ne soit pas plus connu, financé par le ministère qui a pour objectif de permettre aux PME et ETI d'identifier les risques numériques liés à leur activité, d'évaluer le niveau de protection de leurs systèmes d'information, de

détecter les failles éventuelles et d'accompagner la mise en œuvre, le cas échéant, d'un plan de sécurisation.

Mesdames et messieurs,

La signature de cette convention n'est pas une fin, c'est au contraire un début, celui d'une aventure collective animée par la volonté d'exceller dans le cyber, surtout de connaître la menace sous toutes ses formes pour savoir comment la combattre. Cette quête du sommet, cette ardeur à l'effort, c'est le moteur de notre défense. C'est avec cette énergie, avec votre expertise et tous vos talents que nous pourrons construire une cyberdéfense à la hauteur pour protéger nos systèmes mais aussi tous nos concitoyens.

Merci à tous et au travail !