Intervention de Monsieur Bernard Cazeneuve,

Président de l'IDEF,
ancien Premier ministre
à la visioconférence du 1er décembre 2020

Merci d'abord infiniment à vous tous pour votre participation à ce colloque, à cette conférence dans laquelle l'IDEF a souhaité s'impliquer.

Je remercie d'ailleurs beaucoup le secrétaire général de l'IDEF, le professeur Barthélémy Mercadal, qui, depuis beaucoup d'années, consacre une belle énergie au fonctionnement de notre institut et contribue à travers ses travaux au rayonnement du droit continental.

Je voudrais à mon tour, après cette synthèse que vous venez de faire et qui rend compte des travaux que j'ai conduits tout au long de nos débats, dire quelques mots sur les enjeux de la cybercriminalité, tels qu'ils résultent de l'expérience qui fut la mienne dans d'autres responsabilités que celles que j'exerce désormais professionnellement comme avocat, puis à la tête de quelques organisations Think Tank comme le Club des juristes ou comme l'IDEF. J'ai eu dans mes fonctions de ministre de l'Intérieur à rencontrer les dangers, les risques, les menaces, que présente à nous la cybercriminalité. Et vous avez choisi aujourd'hui de traiter plus particulièrement du lien qui existe entre le risque cyber et la crise sanitaire à laquelle nous sommes confrontés. Et vous me permettrez, par souci de complémentarité avec l'ensemble des sujets que vous venez d'évoquer de façon très cohérente, très globale, de donner mon point de vue sur le lien qui peut exister d'un point de vue de politique publique entre cette crise sanitaire et les menaces cyber qui résultent de l'activité de groupes criminels, qui agissent au plan international, mais pas seulement, puisque nous savons que des États utilisent des moyens cyber à des fins d'affirmation soit d'outils de coercition, soit en vue d'exercer des pressions sur tel ou tel État, avec lesquels ils sont dans des relations diplomatiques plus ou moins fluides.

Le premier point sur lequel je voudrais insister, c'est sur ce que vous avez sans doute appelé pendant le débat, je n'y ai pas participé en totalité pour des raisons qui tenaient aux contraintes de mon agenda, mais la cyber coercition est devenue un élément, un outil de pression exercée par certains États sur d'autres. Et cela s'est traduit au cours des dernières années par la découverte, par les services de renseignement, les services de police, par les industriels eux-mêmes, de la pose d'implants par des services de puissances étrangères, dans des entreprises et notamment dans des entreprises du secteur énergétique. Ces implants n'ayant pas vocation à engendrer immédiatement un désordre informatique, mais devant être interprétés comme autant de signaux de la capacité d'un certain nombre d'États de nuire au bon fonctionnement d'autres États plus ou moins amis, en opérant sur les systèmes informatiques d'opérateurs d'importance vitale des pressions, en engendrant des dysfonctionnements qui peuvent être paralysant de l'économie ou de secteurs très stratégiques de pays entiers, comme cela fut le cas pour les implants découverts dans les entreprises énergétiques. Ça a été le cas en France. Ça a été le cas en Allemagne. Et il n'est pas nécessaire de s'attarder sur la signification de ces découvertes. On comprend très bien qu'il s'agit, pour un certain nombre d'États, de faire pression sur d'autres, de manière à apporter témoignage d'une capacité de nuisance. Et si on prend cet exemple de la

cyber coercition, qui est destinée en représailles à des actions ou des prises de positions diplomatiques prises par tel ou tel pays, de faire peser sur ce pays une pression par la mise en perspective de ce que pourrait être une cyber attaque.

On voit bien, si on relie cette question à celle de la crise sanitaire, comment la percolation, dans une même temporalité, de la crise sanitaire et de l'attaque cyber, pourrait occasionner un immense désordre dans des pays qui mobilisent à la fois l'administration régalienne de l'État, l'administration de la santé, les hôpitaux, pour faire face à une crise majeure qui, bien entendu, perturbe énormément les populations pour des raisons qui tiennent à l'impact, sur la santé des citoyens, de ces crises et pour des raisons qui tiennent aussi aux conditions dans lesquelles, pour affirmer leur capacité de résilience, les sociétés s'organisent en mettant parfois en cause un certain nombre de libertés individuelles pour faire face à ces crises. Donc, si on devait ajouter à la crise sanitaire, aux contraintes qu'elle fait peser sur les sociétés, une contrainte résultant de l'utilisation par certains États des maintiens de la cyber coercition, on aurait là un tableau assez sinistre et assez préoccupant de ce que pourrait être le risque cyber.

Le risque cyber peut également résulter, vous l'avez dit, et vous avez eu raison de souligner en prenant de multiples exemples sur ce qu'ont pu être les comportements d'organisations criminelles pendant la crise sanitaire, le risque cyber peut résulter aussi de ce que sont capables d'engendrer comme désordre des organisations criminelles internationales qui utilisent la cyber industrie ou les cyber moyens comme un moyen de pression diplomatique, mais qui les utilisent comme l'instrument de la commission d'infractions pénales extrêmement graves, organisées par des groupes criminels de dimension internationale, très difficiles à appréhender parce que organisés au plan mondial et procédant par des techniques qui ont été j'imagine évoquées aujourd'hui, vous les avez évoquées dans tous les cas dans votre conclusion. On bloque complètement le fonctionnement d'organisation et on engage des processus de demandes de rançon, c'est ce qu'on appelle le rançongiciel, qui sont destinés à récupérer des sommes considérables sur des opérateurs dont l'activité a été totalement bloquée par l'intervention de ces groupes criminels qui peuvent agir à la fois sur des administrations de l'État, sur des opérateurs d'importance vitale, qui peuvent être des hôpitaux, qui peuvent être des administrations régaliennes, qui peuvent être aussi des entreprises privées intervenant dans un secteur stratégique, celui de l'énergie, celui des transports. Et on voit la manière dont ces groupes peuvent bloquer le fonctionnement d'un pays et essayer d'obtenir des administrations ou des institutions publiques ou privées sur lesquelles ils ont opéré, des sommes considérables en contrepartie du déblocage de la situation qu'ils ont eux-mêmes contribué à engendrer par la mobilisation de moyens hautement répréhensibles.

Là aussi, je vous laisse imaginer ce que serait la situation si nous devions, en même temps que nous sommes confrontés à une crise sanitaire, que nous sommes confrontés à une crise terroriste, si nous devions nous trouver face à des organisations criminelles internationales qui, pour atteindre leurs objectifs politiques, s'il s'agit de groupes terroristes, viendraient procéder au blocage de secteurs entiers d'un pays, contribuant ainsi à ajouter de la désorganisation au traumatisme occasionné par la crise sanitaire, empêchant les pays, et notamment les démocraties, de faire la démonstration de leur capacité de résilience. Le sujet serait non seulement un sujet de fonctionnement normal et régulier des pouvoirs publics dans un contexte particulièrement [vécu], mais ce serait un problème politique, dans la mesure où le

blocage complet du système démocratique ne manquerait pas d'engendrer des fracturations au sein de ce système, des formes de contestation de la légitimité du pouvoir, en raison de l'impossibilité dans laquelle il serait de faire face à la crise et de trouver les moyens de la surmonter. Et nous serions ainsi confrontés à la fois à une crise économique, à l'ensemble de menaces s'agrégeant dans un pays, à une crise de fonctionnement de l'État et de la société extrêmement préoccupant.

Il y a un troisième élément, sur lequel je voudrais insister, qui est un autre élément de la cybercriminalité, qui est l'utilisation par des groupes idéologiques qui ont des objectifs politiques qui sont très orthogonaux, ce que sont les valeurs et les principes démocratiques, et qui utilisent les moyens informatiques et numériques pour faire passer de fausses informations, pour organiser des propagandes, pour engendrer des processus d'endoctrinement qui ont vocation à créer des phénomènes de rupture, de confrontation, de violence dans la société, et notamment dans la société démocratique. Nous avons vécu ça, d'ailleurs je sais qu'il y a des collaborateurs du ministère de l'Intérieur qui ont participé à cette conférence et qui sont encore présents. Je ne peux pas ne pas me souvenir avec eux de ce que furent les moments auxquels nous avons dû faire face lorsque la crise terroriste a atteint dans les années 2015-2016 son paroxysme.

Nous avions été très frappés en 2015-2016 de constater que, alors que les attentats terroristes avaient fait subir au pays un choc profond, et notamment en janvier, en novembre 2015, puis en juillet 2016, le nombre de messages qui avaient été diffusés dans la continuité de ces attentats, appelant et provoquant au terrorisme, à l'antisémitisme, à la haine, parfois la haine anti musulmans, s'étaient propagés et nous avions pu constater, par la plateforme PHAROS de la direction centrale de la police judiciaire, une augmentation de près de 70 % du nombre de messages appelant et provoquant au terrorisme. De la même manière nous savons, par les études qui sont à notre disposition, que le processus de radicalisation qui est organisé par les groupes terroristes, par internet, parvient à atteindre sa cible beaucoup plus que les prêches qui sont dispensés par des imams radicalisés dans les mosquées ; 90 % de ceux qui se sont radicalisés au cours des dernières années se sont radicalisés essentiellement par internet. Ce qui a donné naissance à ce qu'un certain nombre de chercheurs français, je pense notamment à Gilles Kepel, ont appelé un terrorisme réticulaire, c'est-à-dire un terrorisme qui naît spontanément dans les territoires, sans que ceux qui se laissent aller à l'endoctrinement détecté, engagés sur des théâtres d'opérations terroristes et qui, par le biais d'une propagande numérique, une cyber propagande, très efficace, se radicalisent, passent à l'acte, sans nécessairement d'ailleurs que les services de renseignement soient en situation de les détecter toujours, puisque on a vu, par exemple pour l'attentat qui a été perpétré contre le père Hamel et les fidèles à Saint-Etienne-du-Rouvray, ceux qui avaient préparé ces attentats, les avez préparés par l'utilisation de moyens cryptés. Et si on n'utilise pas, nous-mêmes, un certain nombre de moyens technologiques pour identifier ces messages qui sont annonciateurs de la commission d'attentats avant qu'ils ne soient commis, alors nous passons à côté des personnes qui sont susceptibles de passer à l'acte. Et, là aussi, chaque incapacité des services à prévenir un attentat engendre un débat démocratique bien légitime sur les failles des services de renseignement. Et ce débat est un débat qui engendre mécaniquement une perte de confiance. C'est la raison pour laquelle nous avons dû moderniser les règles législatives relatives au renseignement, en adoptant la loi de juillet 2015 relative au

renseignement, et qui nous a permis de moderniser considérablement les techniques de renseignement, pour faire face, précisément, à ces groupes criminels qui intervenaient dans le domaine de la cybercriminalité. De la même manière que, au plan européen, nous avons été amenés à renforcer la coopération au sein de l'EUROJUST, pour mieux combattre la cybercriminalité à l'échelle du continent, et nous avons été amenés, lorsque nous avons adopté la directive relative au trafic d'armes, après les attentats de novembre 2015, au plan européen, à intégrer la dimension cyber, parce que beaucoup de ces trafics intervenaient sur le darknet à l'initiative de groupes criminels, situés plus particulièrement en Europe de l'Est, mais pas seulement, et qui alimentaient les réseaux terroristes par l'utilisation de moyens cyber. Donc on voit qu'il y a la cyber coercition, il y a la cybercriminalité. Elle prend des formes extraordinairement diverses. Pendant la crise sanitaire, elle a pu conduire aussi à des opérations de fraude ou à des opérations destinées à abuser les consommateurs, je n'y reviens pas parce que je crois que ça a été évoqué assez précisément pendant les débats, mais enfin la cybercriminalité a des visages très divers et elle conduit aussi à l'utilisation des moyens numériques à des fins de la réalisation d'objectifs politiques.

Une fois que l'on a dit cela, cyber coercition par les États, cybercriminalité par les organisations criminelles internationales, *fake news* et utilisation d'internet à des fins d'endoctrinement ou de la commission d'actes violents, se pose la question de savoir comment on fait. Parce que ce qui est de nature à éviter les drames, c'est la coopération entre les différents services en charge. Je ne veux pas être désagréable aux officiers de la gendarmerie qui sont ici présents, ni aux hauts responsables du ministère de l'Intérieur et de la Justice qui nous ont fait l'honneur de participer à ce colloque, mais je crois que l'on peut dire que la coopération et la montée en puissance des outils étatiques s'est considérablement développée au cours des dernières années, contribuant à mieux garantir la protection contre le risque cyber, notamment par la conjonction de 3 interventions, d'abord l'ANSSI qui est responsable de la protection des systèmes publics, civils et des opérateurs d'importance vitale, le COMCYBER qui est chargé de la protection du système du ministère des Armées, qui intervient simplement pour le compte du ministère des Armées, en riposte des éléments produits ici ou là, et la direction technique de la DGSE qui, elle, intervient à sa manière pour essayer de bloquer les choses, et puis il y a toutes les entités cyber des ministères qui assurent leur rôle dans le domaine de leurs compétences. Je sais que la gendarmerie est très puissamment armée, la plateforme PHAROS au sein du ministère de l'Intérieur joue son rôle dans le domaine de la lutte contre la cyber haine etc. Mais on voit bien que nous avons un double défi qui pour l'instant n'est pas pris à la hauteur de la menace qui se présente à nous.

Le premier défi, c'est la coordination de l'ensemble des moyens qui peuvent être mobilisés par les grands acteurs privés qui interviennent dans des secteurs stratégiques. J'ai parlé de l'énergie, des transports et les grandes administrations de l'État. Et je lance là quelques éléments de réflexion prospective. Et je me pose la question de savoir si nous n'aurions pas intérêt, dans le domaine de la lutte contre la cybercriminalité, à avoir un coordonnateur à la lutte contre la cybercriminalité qui pourrait travailler en très étroite liaison avec le coordonnateur en charge du renseignement pour essayer de couvrir la totalité de la gamme des menaces qui se présentent à nous et de mettre de la cohérence dans les politiques publiques destinées à résister à ce type de menaces. Je pense que la coordination de l'ensemble des acteurs est absolument

fondamentale pour atteindre un meilleur niveau d'efficacité. L'ANSSI pourrait bien entendu jouer dans ce dispositif un rôle de pierre angulaire, compte tenu des compétences qui sont les siennes, mais le rôle majeur de l'ANSSI, qu'il faut saluer parce qu'il est absolument remarquablement orchestré, pourrait être complété d'un rôle de coordination nationale qui permettrait à l'ANSSI de pouvoir, dans son rôle pierre angulaire, être accompagnée par un certain nombre d'acteurs publics et privés.

Le deuxième élément sur lequel je souhaiterais insister, c'est sur la nécessité d'essayer de créer les conditions d'une base technologique et industrielle renforcée en matière de lutte contre le risque cyber. Nous avons beaucoup de start-up, beaucoup de PME, quelques ETI, mais nous avons une base industrielle qui est aidée de façon trop complexe avec des acteurs multiples. Et si nous avions la possibilité sur le plan industriel de faire plus et mieux, ce serait incontestablement utile et efficace.

Enfin, il y a un troisième point qui paraît fondamental, c'est d'essayer de développer, sur ces questions qui sont stratégiques, la coopération européenne. Et je crois que tout ce qui peut se faire sur le plan européen en matière cyber est utile. Nous avons vu d'ailleurs, sur un sujet qui est connexe, qui est celui de la protection des données personnelles, à quel point le règlement européen qui a été adopté était efficace, et efficace y compris dans la relation extra territoriale que l'Europe peut avoir avec un certain nombre d'autres continents ou d'autres puissances, je pense notamment aux États-Unis, et nous devrions pouvoir nous inspirer de ce qui a été fait sur la question des données pour essayer de renforcer la coopération européenne sur la question des menaces.

Voilà quelques-unes des réflexions que je voulais partager avec vous à l'occasion de la conclusion de vos débats pour essayer d'une part de participer à la synthèse dans laquelle vous vous êtes engagés et vous dire à quel point je suis plein de gratitude pour votre implication dans ces travaux, et puis essayer aussi de lancer quelques ponts vers l'avenir, en termes de réflexion prospective, à partager avec l'ensemble des acteurs concernés sur un sujet dont je sais qu'il est absolument stratégique pour la sécurité des puissances économiques et des pays. J'en ai fait l'expérience lorsque que j'étais ministre de l'Intérieur et notamment lorsqu'une chaîne de télévision a été prise d'assaut par une cyberattaque, avec le drapeau de Daesh s'affichant sur l'écran de cette chaîne de télévision, laissant à penser que nous étions confrontés à une attaque terroriste, alors que, avec le temps, il est apparu que cette attaque était d'une autre nature et procédait d'une manipulation dont les cybercriminels sont aussi capables.

Merci à vous