Numérique

Présentation de la stratégie internationale de la France pour le numérique à thecamp – Discours de M. Jean-Yves Le Drian, ministre de l'Europe et des affaires étrangères

Aix-en-Provence, 15 décembre 2017

Mesdames et Messieurs, chers amis,

D'abord, merci pour vos témoignages et expériences toniques, stimulantes et décloisonnantes sur nos nouvelles réalités.

Je suis heureux que vous ayez accepté de répondre à mon invitation aujourd'hui. Les différents secteurs d'activité dans lesquels vous travaillez prouvent, s'il en était encore besoin, combien nous avons besoin d'une vision cohérente et intégrée de la diversité des enjeux numériques. Combien nous avons également besoin d'un cap et d'objectifs clairs pour agir ensemble dans un domaine qui conditionne très directement les succès présents et à venir de notre pays et ceux de l'Europe. C'est le but de la stratégie que je vous présente aujourd'hui.

Les uns et les autres, nous avons découvert aujourd'hui ce lieu magnifique. Je tiens tout d'abord à remercier chaleureusement les équipes de *thecamp* pour leur accueil et leur enthousiasme.

Ce lieu, nous le devons au rêve et à la détermination d'un homme, Frédéric Chevalier, disparu brutalement il y a quelques mois et à qui je veux rendre hommage. Entrepreneur visionnaire, il a voulu créer un lieu à l'image des promesses que porte le monde numérique, un lieu qui puisse former des cadres aux changements induits par la révolution numérique, inviter des jeunes talents du monde entier à réfléchir et créer ensemble, instiller dans l'esprit des plus jeunes le goût de l'innovation par le jeu, fournir à des start-ups les moyens de se développer en créant autour d'elles un écosystème qui favorise la réussite, permettre enfin aux collectivités locales partenaires d'expérimenter des idées et des projets avant qu'ils ne donnent lieu à de véritables politiques publiques.

Dans ce choix de la Provence, il y avait bien sûr l'amour d'un homme pour son territoire. A quelques encablures de la Sainte-Victoire, je me rappelle aussi que c'est au contact de ces paysages que Cézanne, et tant d'autres créateurs à sa suite, ont voulu inventer une nouvelle modernité, styliser une nouvelle manière de percevoir et de s'orienter dans le monde.

C'est une ambition semblable qui nous rassemble aujourd'hui, celle de définir les contours de la modernité numérique que nous souhaitons pour notre pays, d'affirmer une certaine idée du monde numérique auprès de nos partenaires internationaux. L'écrin futuriste de *thecamp* en donne une image : je regarde *l'ouverture* de ces lieux, la *transparence* de son architecture bâtie pour favoriser la *circulation*, *l'échange*

et la *coopération*, et j'y vois en réalité l'image matérielle des valeurs qui sont pour la France indissociable de la révolution numérique et de ce qu'elle apporte à nos concitoyens.

Thecamp, c'est aussi la démonstration que le modernisme le plus assumé peut être en harmonie avec un environnement naturel préservé. J'y vois, là aussi, la preuve que la révolution numérique nous donne des instruments assurer la transition écologique de nos sociétés.

I. Situation de la mondialisation numérique

1. Une rupture historique

L'émergence d'un espace numérique mondial constitue une rupture comme il en existe peu dans l'histoire de l'humanité. Au siècle passé, l'homme a conquis les airs et les abysses, il a porté ses rêves jusque dans l'espace. Mais la révolution la plus extraordinaire - elle est sans équivalent dans notre histoire - est d'avoir créé un nouveau milieu pour communiquer, produire, consommer, échanger, s'informer, apprendre, se divertir. Cette révolution globale a peu à peu gagné et bouleversé toutes les sphères de l'activité humaine en faisant de la digitalisation un facteur de mondialisation accélérée. Les révolutions les plus considérables sont celles qui s'imposent par leur évidence, au point de rendre difficilement imaginable le monde tel qu'il était avant leur éclosion. Je pense à notre jeunesse, la génération des *digital natives* pour qui l'espace numérique est un environnement naturel et familier.

Qui aurait pu imaginer cela en 1969, lorsque le premier message fut échangé entre les universités de UCLA et de Stanford sur le réseau de l'ARPANET ? Alors que la révolution numérique est en pleine accélération, qui pourrait aujourd'hui prédire avec certitude la manière dont elle transformera encore notre existence dans les décennies à venir ? Nous ne sommes qu'au début d'une nouvelle ère, nous le pressentons tous, comme nous le laisse déjà voir l'intelligence artificielle et les objets connectés.

2. Le risque d'un monde numérique dérégulé, dangereux et fermé

Vous le savez, je suis un réaliste. Dans mes fonctions, je constate chaque jour que notre époque est la plus incertaine et la plus instable depuis la fin de la guerre froide. Et je fais entrer dans mon diagnostic les bouleversements induits par l'irruption du numérique comme nouvel espace de conduite des relations internationales.

En prenant un peu de champ, je dirai que l'espace numérique s'est développé selon une double tension qui atteint aujourd'hui son paroxysme : tension d'une part entre la promesse d'ouverture à l'échelle globale et les vulnérabilités nouvelles qui en résultent ; tension d'autre part entre la fin des barrières à l'entrée, qui facilite en théorie l'émergence de nouveaux acteurs économiques, le développement de nouveaux besoins sociaux et de nouveaux marchés, et la possibilité que donne

Internet à des acteurs économiques dominant d'établir des positions hégémoniques qui nuisent à la concurrence et donc, à terme, à l'innovation.

L'espace numérique est porteur de progrès ; il peut donner à nos valeurs démocratiques un nouveau souffle, mais nous faisons en même temps désormais face à un risque, celui d'un monde numérique manipulé contre les vertus d'ouverture dont il devait être le garant.

a. Les risques de l'hégémonie économique

La révolution numérique a bouleversé les structures mêmes de l'économie globalisée. Elle a permis d'ouvrir le champ de la compétition économique, en raison de la réduction des coûts et de la suppression des intermédiaires. De nouveaux marchés et de nouveaux acteurs ont pu émerger, et avec eux de nouveaux modèles économiques. Dans le domaine économique, nous faisons pourtant face à trois risques.

D'abord, dans le même temps de cette émergence de nouveaux acteurs, les grands groupes américains et chinois, ont su consolider des positions monopolistiques, en s'appuyant notamment sur des effets de réseaux et sur une masse critique de données. Ces instruments leur permettent aujourd'hui non seulement d'améliorer leurs services mais aussi d'empêcher toute concurrence. Ils peuvent agir ainsi grâce au contrôle qu'ils exercent de fait sur les nouvelles routes numériques, par les politiques de rachats agressives auxquelles ils se livrent, ou par la prédation par les prix qu'ils pratiquent.

Des Empires se sont bâtis dans l'Histoire sur la domination des routes terrestres ou maritimes. De nouveaux Empires tentent aujourd'hui de s'imposer par le contrôle des flux numériques.

Deuxièmement, le développement d'acteurs dominants pose une autre question critique, s'agissant cette fois de la résilience d'Internet. Son extension mondiale garantit que si une de ses parties est compromise, l'ensemble du réseau résiste. Il n'a donc pas de point de fragilité réel. Mais ce modèle est en train d'être remis en cause par l'émergence d'acteurs qui, en centralisant une quantité gigantesque d'information, deviennent eux-mêmes des points individuels de défaillance (*SPOF* : *single point of failure*). C'est un signe des contradictions qui traversent ce secteur : ils nous offrent des outils de communication sans précédent mais dans le même temps, a capacité à désinformer à grande échelle ne serait pas atteignable sans les géants de l'internet. Il y a donc là un enjeu particulier de régulation.

Le troisième risque d'un tel monopole économique, c'est celui de l'hégémonie culturelle et idéologique. Je remarque par exemple que la gouvernance technique de l'internet ne laisse pour l'heure que peu de place au multilinguisme, alors même que le numérique nous offre des ressources extraordinaires de promotion et de diffusion des productions culturelles à l'échelle mondiale Nous assistons ainsi à la constitution de zones linguistiques séparées les unes aux autres. Des tendances au repli, au cloisonnement et à la fermeture se font jour. Ce n'est pas le choix de la France. Nous

optons pour un multilinguisme ouvert. Je pense notamment à nos projets concernant le rayonnement de la francophonie. Aujourd'hui 3% de l'internet est francophone. En 2050, ce sera 8%, grâce à la croissance démographique en Afrique francophone. C'est un atout dont nous devons nous saisir.

b. Les inégalités numériques

Dans le domaine économique, nous devons aussi être conscients que la mondialisation numérique n'est pas homogène : le défi de l'inclusion est devant nous parce que la révolution numérique laisse encore sur le bord du chemin une part importante de la population mondiale.

Les inégalités propres à l'ère numérique sont de plusieurs ordres. La première d'entre elle, la plus structurelle aussi, c'est une inégalité d'accès entre ceux qui bénéficient de la couverture réseau et ceux qui vivent dans des « déserts numériques » ; la seconde est une inégalité de maîtrise, entre ceux qui se sont appropriés les outils numériques ou qui ont la possibilité de s'y former, et les autres qui sont exclus de ce cycle de formation et de développement ; la troisième est une inégalité de conception, entre ceux qui participent au développement des outils numériques et les autres qui se trouvent ainsi dans un état de dépendance vis-à-vis du progrès technologique.

Je note d'ailleurs que les acteurs du numérique sont eux aussi concernés par les inégalités de genre : les femmes sont encore trop peu présentes dans les écosystèmes numériques, mais aussi dans les disciplines scientifiques qui permettent d'accéder à ces métiers. Je tiens d'ailleurs à saluer des initiatives comme celle de l'association « jamais sans elles » qui place cette question au cœur de la transformation numérique de notre société. C'est la raison pour laquelle j'ai décidé de la rejoindre.

c. L'espace numérique : nouveau domaine de conflictualité

Je le disais il y a un instant, l'architecture de l'internet a été pensée et construite dans une logique d'ouverture et non de sécurité. Il en résulte pour l'ensemble des acteurs du cyberespace des vulnérabilités nouvelles et l'apparition de formes inédites de conflictualité. En témoigne l'augmentation exponentielle des attaques informatiques à travers le monde. Leurs cibles sont de plus en plus variées : elles peuvent toucher les infrastructures de défense des Etats, les services publics, les entreprises et les citoyens eux-mêmes. La dernière décennie l'a amplement prouvé, depuis l'attaque contre l'Estonie en 2007 jusqu'à tout récemment, avec *WannaCry* et ses conséquences sur les hôpitaux londoniens en 2017 ; je pense également au piratage des messageries officielles allemandes en 2015 et britanniques en 2017, ou encore au vol massif de données subis par différentes entreprises, y compris françaises. Et je n'oublie pas, bien sûr, l'attaque qui a pris pour cible TV5 Monde en 2015.

Les cibles sont diverses ; les attaquants le sont aussi : ils peuvent être de nature étatique, et nous assistons dans ce domaine à une prolifération d'un nouveau type, celle des forces cyber dont les stratégies ne sont pas toutes défensives. Je constate d'ailleurs une aggravation de la nature même de la menace. En quelques années, nous sommes passés d'une logique de captation d'information et d'espionnage à des

attaques d'une autre nature. Les capacités numériques sont désormais utilisées comme une arme au sens strict, avec pour finalité la paralysie ou la destruction d'infrastructures vitales et leurs conséquences sur l'existence de nos concitoyens J'ai eu l'occasion, il y a un an presque jour pour jour, de présenter les principaux principes de notre stratégie de cyberdéfense. Celle-ci devra évidemment, dans les mois qui viennent, continuer d'être précisée, à mesure qu'évoluent les menaces, mais aussi pour que nos agresseurs potentiels puissent connaître les conséquences d'actions éventuelles contre nous. C'est l'enjeu de la revue cyber à venir.

A cette première catégorie d'assaillants étatiques, s'ajoute un nombre de plus en plus important d'acteurs non étatiques ; ils forment ce qu'il faut bien appeler un véritable marché de l'ingérence : la constitution de « fermes à troll », le rôle des mafias ou des hackeurs, parfois pilotés par les Etats, en sont les signes les plus visibles.

3. Pour un ordre numérique coopératif

Nous sommes à la croisée des chemins : le numérique, ce sont aujourd'hui des opportunités, des innovations synonymes de croissance, de libertés et de pratiques nouvelles. Mais cette transformation globale comporte aussi des risques de déséquilibres et de tensions internationales. Ici comme ailleurs, les crises surviendront si nous ne remédions pas au manque de coopération dont souffre aujourd'hui l'espace numérique.

Il n'entre aucun fatalisme dans ce diagnostic. Au contraire, ce constat indique clairement le défi que nous avons à relever : nous prémunir des risques que je viens de caractériser afin de créer un ordre numérique juste, favorable au développement de chacun.

Nous ne voulons pas nous laisser enfermer dans une alternative simplificatrice entre la fermeture et le laissez-faire ; nous voulons dessiner une autre voie, faite d'équilibre entre ouverture et protection, coopération et liberté d'action, une voie adaptée à la préservation de la paix et au maintien de notre puissance à l'âge numérique.

Le sens de la stratégie internationale de la France que je vous présente aujourd'hui est précisément de promouvoir un ordre numérique international coopératif, avec des règles partagées, gage de confiance mutuelle : c'est la condition de la stabilité internationale. Et c'est pour cela justement que l'ère numérique demande une action diplomatique renouvelée, capable d'associer, là où c'est nécessaire, la société civile, le secteur privé et le monde de la recherche afin de définir ensemble des formes de régulation originales adaptées à l'évolution du monde numérique, qu'il s'agisse de mécanismes d'auto-régulation ou de co-construction de la norme.

Cette créativité multilatérale, réaliste et pragmatique, c'est la méthode que la France souhaite porter afin de définir le monde numérique que nous souhaitons et le rôle que la France et l'Europe doivent y jouer dans les décennies à venir. Un monde où notre sécurité est garantie, où nos droits fondamentaux sont préservés et où nos acteurs économiques sont compétitifs.

C’est ce que propose la stratégie internationale pour le numérique : elle est le résultat d’un travail collectif de concertation et de consultation publique mené par le Ministère de l’Europe et des Affaires étrangères, en lien avec l’écosystème numérique et les différents services de l’Etat concernés. Je veux spécifiquement remercier Marine Guillaume, Justin Vaïsse et David Martinon, qui y ont travaillé depuis plusieurs mois.

II. La stratégique internationale pour le numérique

Mesdames et Messieurs,

Cette stratégie veut promouvoir une gouvernance adaptée aux transformations majeures que provoque la révolution numérique.

1. Gouvernance et régulation

a. Pour une gouvernance multipartite, transparente et inclusive

Pour être légitime, la gouvernance du numérique doit d’abord répondre à des conditions de démocratie et de représentativité.

Depuis la création de l’ICANN en 1998, la France a constamment appelé à la mise en œuvre d’un modèle de gouvernance multipartite, transparente et inclusive, prenant en compte les responsabilités générales des Etats et la nécessité de contrebalancer les intérêts économiques des grandes entreprises par la prise en compte de l’intérêt public mondial. J’ajoute que la France continuera à défendre le principe de la neutralité de l’Internet, alors que s’exprime aujourd’hui des volontés de la remettre en cause.

b. Porter nos efforts à l’échelle européenne

Pour être entendu, il importe de construire en amont des positions coordonnées qui pourront ainsi peser concrètement. C’est pourquoi nous invitons les acteurs numériques français et européens à renforcer leur engagement à nos côtés dans l’ensemble des instances de gouvernance, afin de faire valoir la vision et les intérêts que nous partageons.

L’horizon de cette stratégie est européen. C’est en effet le niveau critique pour peser réellement dans les négociations que nous aurons à conduire, avec les Etats comme avec les acteurs privés. Seule l’Union européenne aura le poids nécessaire pour incarner et porter cette vision à l’échelle internationale.

c. L’enjeu de la protection et de la maîtrise personnelle des données

C'est tout particulièrement le cas s'agissant des données personnelles. Elles sont le carburant de la nouvelle économie. Leur protection et leur maîtrise sont donc une priorité de l'effort diplomatique que nous souhaitons mettre en œuvre. Ces principes sont à la base du règlement général sur la protection des données qui entrera en vigueur le 25 mai 2018, à l'échelle européenne. Il permet aux citoyens de contrôler les données qui les concernent, un droit qui oblige d'ailleurs autant les acteurs économiques privés que les services de l'administration. Ce règlement repose sur plusieurs principes, que je veux rappeler : d'abord la loyauté, c'est-à-dire le traitement licite et transparent des données ; ensuite, la limitation des données collectées pour une finalité précise et légitime; bien sûr l'exactitude des données et la limitation dans le temps de leur conservation ; enfin, l'intégrité et la confidentialité, principes qui doivent garantir la sécurité des données. Et ces principes emportent avec eux des droits : droits d'accès, de rectification et d'effacement des données personnelles.

Notre objectif est donc bien de promouvoir de façon aussi large que possible un modèle européen d'organisation dont nous souhaitons faire la référence mondiale en la matière.

Cet effort, nous le portons dans deux directions. Premièrement, le domaine économique. Deuxièmement, les enjeux de sécurité propres au numérique.

2. Axe économique

Dans le domaine économique, nous avons quatre impératifs : la modernisation ; la régulation ; la protection ; le développement.

a. Moderniser notre économie : la France, pôle d'excellence numérique

Ce que nous voulons tout d'abord, c'est faire de la France un pôle d'excellence numérique. Ce défi de la modernisation et de la transition numérique de notre économie suppose de créer un écosystème favorable à l'innovation et à l'investissement. C'est l'objectif recherché par la structuration de notre filière numérique avec la French Tech. Je pense également au French Tech ticket et au French Tech visa, qui permettent aux entrepreneurs étrangers de s'installer très facilement et très rapidement en France pour développer leur projet. Je suis heureux de saluer leurs représentants qui m'accompagnent aujourd'hui.

En offrant des instruments à nos entreprises pour conquérir de nouveaux marchés à l'étranger, le numérique est également un levier fondamental pour la diplomatie économique de notre pays dont j'ai la responsabilité. A cet égard, les 7 recommandations du Conseil National du Numérique, pour numériser les PME constituent une base de travail pour combler les retards pris dans ce domaine. C'est l'objectif de la Mission confiée par le secrétaire d'Etat au Numérique Mounir Mahjoubi à Philippe Arraou *« pour (…) la transformation digitale des TPE-PME »*.

b. Protection dans le domaine économique

- Concurrence et fiscalité

Pour que cette ambition économique soit viable, nous devons aussi garantir des règles du jeu équitables en matière de concurrence et de fiscalité. En effet, les acteurs européens souffrent aujourd'hui d'une situation qui leur est défavorable, en raison notamment de l'optimisation fiscale agressive à laquelle se livrent les grandes plateformes.

De façon globale, l'activité économique numérique pose un défi aux critères classiques d'imposition des entreprises. De la valeur est créée, des transactions sont réalisées sur le territoire national et européen sans que la présence physique des entreprises soit nécessaire pour cela. Pour mémoire, je rappelle qu'entre 2013 et 2015, la perte fiscale pour l'Union européenne est estimée à 5,4 milliards d'euros. Je constate d'ailleurs que les choses bougent dans ce domaine. Ces comportements sont enfin sanctionnés par Bruxelles avec l'amende de 2,4 milliards d'euros adressée à Google pour abus de position dominante ou le redressement fiscal d'Amazon qui s'élève à 250 millions d'euros.

Toutefois ces mesures de redressement ne sont qu'un aspect de la solution. Il nous faut encore une régulation véritable. Pour être efficace, comme je le disais, il faut la porter à l'échelle européenne. La France travaille donc à des projets de taxation avec pour objectif que le caractère immatériel de l'activité numérique n'échappe pas à une imposition adaptée. Elle pourrait prendre pour objet les bénéfices ou le chiffre d'affaires.

- Répartir la valeur de façon équitable

De façon globale, la révolution numérique suppose que nous modernisions un certain nombre d'instruments juridiques afin de garantir une répartition équitable de la valeur produite. Je pense notamment à la modernisation du droit d'auteur, en cours de révision à l'Union européenne. Comme l'a dit le président de la République lors de son discours de la Sorbonne, dans cette Europe du numérique, nous devons défendre partout où elle existe la valeur créée par celui qui crée vraiment, afin de parvenir à une rémunération juste de l'ensemble des auteurs et de toutes les formes de création dans le numérique.

- Protéger des droits fondamentaux des usagers

L'usage que font les plateformes du *big data* exige également une vigilance particulière de la part des pouvoirs publics. Je comprends que les entreprises protègent la propriété intellectuelle de leurs algorithmes. J'aimerais néanmoins savoir quels sont les objectifs qu'elles poursuivent, même généraux, en employant ces instruments mathématiques pour développer leurs activités.

Il y a là une exigence de transparence démocratique et de loyauté, je dirai même un impératif éthique s'agissant des choix sociaux et de la liberté individuelle. Les citoyens ont le droit de comprendre à quoi servent leurs données et les mécanismes de recommandation qui encadrent de fait leur utilisation des outils numériques.

De façon générale, l'idée qui nous inspire est celle d'un équilibre entre la modernisation des usages, la ressource que représente le *big data* pour nos entreprises, les améliorations qu'il permet dans différents domaines, je pense aux progrès que promet l'intelligence artificielle par exemple dans le domaine de la santé, et l'instauration de certaines normes nécessaires à la maîtrise par chacun de ces données personnelles et au respect de sa vie privée.

c. Le numérique, instrument du développement

Enfin, je veux souligner le rôle majeur des capacités numériques dans le domaine du développement économique et humain, et dans celui de l'action humanitaire. Les acteurs du développement présents aujourd'hui le savant bien, le numérique constitue un puissant moteur de croissance inclusive, à la condition de réduire la fracture numérique dont je rappelais les inégalités caractéristiques il y a un instant.

La France s'engage sur ce terrain via le plan numérique et développement. Le président de la République a aussi annoncé dans son discours de Ouagadougou vouloir soutenir les PME africaines à hauteur de 1 milliard d'euros. Le Fonds de soutien qui sera créé permettra notamment, avec l'Agence française de Développement et la Banque publique d'investissement, de soutenir le secteur numérique africain. C'est le sens du programme *Digital Africa* qui permettra d'identifier les start-up africaines les plus prometteuses et accompagnera leur croissance.

3. Axe sécuritaire

Le deuxième domaine dans lequel nous voulons agir, c'est celui de la sécurité et de la stabilité du cyberespace. Nous faisons face, je l'ai rappelé, à la multiplication et à la diversification des cyber-menaces dans un contexte où, je tiens tout de même à le rappeler, 90% de l'internet mondial est réputé non visible. Pour cela, la France doit réussir à s'affirmer comme un acteur leader en Europe, à même de garantir la stabilité stratégique dans le cyberespace et de décourager les agressions visant nos intérêts.

Pour ce faire, nous devons relever quatre défis :
Le premier est de garantir notre autonomie stratégique, et celle de l'Union européenne, y compris dans le cyberespace ; le second est la bonne prise en compte, par les pouvoirs publics comme par les citoyens des risques et menaces informationnelles ; le troisième est lié à l'utilisation d'Internet à des fins criminelles ou terroristes ; enfin, le quatrième est un enjeu collectif de régulation internationale du cyberespace.

a. Autonomie stratégique nationale et européenne

L'exigence d'autonomie pour la France et l'Union européenne s'applique également dans l'espace numérique. Au niveau national, notre autonomie stratégique repose sur une capacité d'appréciation indépendante ainsi que sur une liberté permanente de décision et d'action. Aujourd'hui, cette autonomie est tributaire de la sécurité des réseaux informatiques et des infrastructures sur lesquels elle repose. Préserver les fonctions vitales remplies par ces réseaux et ces infrastructures fait donc partie des intérêts essentiels de la Nation.

C'est pourquoi la stratégie que je présente aujourd'hui prend en compte l'ensemble des enjeux de sécurité du numérique, tant au niveau national qu'européen.

Je suis en effet persuadé que c'est en travaillant à ces deux niveaux, sans les confondre mais sans oublier non plus les liens qu'ils entretiennent, que nous serons à même de garantir notre sécurité et notre souveraineté dans ce domaine. L'objectif d'autonomie stratégique européenne est le gage de notre capacité collective d'initiative et d'action. Les Européens doivent être capables de maîtriser les technologies clés et d'investir dans les domaines d'innovation stratégique, dans celui des technologies de rupture, et le numérique en, fait bien sûr partie.

Dans le demi-siècle à venir, de nouvelles ruptures technologiques dans le domaine du numérique auront très vraisemblablement des conséquences d'importance similaire, voire supérieure, à celles de la première révolution numérique que nous traversons aujourd'hui. Les recherches en matière d'intelligence artificielles laissent déjà présager de changements majeurs susceptibles de faire évoluer les rapports de force à l'échelle mondiale.

D'autres champs, comme l'informatique quantique, sont encore un pari sur l'avenir, mais nous ne pouvons pas nous contenter d'y assister en spectateur, car ces technologies peuvent avoir des conséquences majeures pour notre autonomie stratégique.

Prendre la mesure de ce défi, c'est l'objectif de la mission sur l'intelligence artificielle confiée par le Président de la République à Cédric Villani, comme de la stratégie qui s'en suivra dans les mois à venir.

Nous devons donc adopter une démarche exploratoire résolue, sans ignorer que ces développements technologiques auront à la fois des applications civiles et militaires. Mais pour que ces technologies soient, demain, au cœur de notre outil de défense, il faudra que les enjeux éthiques et juridiques qui y sont liés soient bien pris en compte.

Stratégiques pour notre défense et notre sécurité, ces capacités le sont aussi pour la confiance qu'ont les citoyens européens dans l'écosystème numérique. Seule une synergie des compétences européennes – souvent excellentes en la matière – pourra nous permettre de soutenir la compétition avec les autres acteurs majeurs, publics et privés, engagés dans cette course à l'innovation. Cet effort européen doit compter sur une coopération franco-allemande renforcée. C'est l'ambition des initiatives du Conseil franco-allemand du 13 juillet dernier. C'est également le sens de la proposition du Président de la République de créer, dans les deux ans qui viennent, une « Agence européenne pour l'innovation de rupture ».

De façon générale, une meilleure coordination entre Européens doit permettre d'éviter lacunes et doublons capacitaires. C'est parce que nous serons capable de nous entendre, de joindre et de mutualiser nos forces que nous pèserons véritablement, à la fois sur les enjeux économiques, sécuritaires et juridiques du numérique.

Ces interdépendances librement consenties renforceront la souveraineté de chaque État membre en accroissant les moyens disponibles à l'échelle européenne.

Au niveau européen, cet objectif d'autonomie stratégique se décline autour de trois piliers :

- Premièrement, c'est la condition essentielle de l'autonomie, un pilier technologique. L'Union européenne doit mener une politique industrielle et soutenir une R&D de pointe afin de favoriser le déploiement de technologies et de services numériques, dont la sécurité doit pouvoir être évaluée, afin de construire un avantage concurrentiel au profit des offres européennes. A ce titre, l'Union européenne doit s'affirmer comme une autorité de certification à part entière des produits et des services informatiques.
- Deuxièmement, un axe réglementaire. L'Union européenne doit mener une politique extérieure capable de définir des réglementations qui prennent en compte à la fois les exigences de compétitivité et les potentialités du numérique et l'impératif de protections des citoyens, des entreprises et des Etats-membres, comme je l'indiquais il y a un instant, et ceci en conformité avec nos valeurs communes.
- Troisième et dernier pilier, un pilier capacitaire afin de soutenir, en s'appuyant sur des savoir-faire européens, le développement des capacités de cyberdéfense, dans le domaine public comme pour les acteurs privés.

Dans ce domaine, nous avançons. Je pense au pôle d'excellence cyber de Rennes, qui bâtit des partenariats avec des pays qui souhaitent s'appuyer sur les compétences de haut niveau qui y sont présentes. Je pense à notre action pour conforter la souveraineté de nos partenaires dans ce domaine, à l'image de ce que nous faisons avec le projet d'implantation à Dakar d'une Ecole Nationale à Vocation Régionale (ENVR) dont j'ai annoncé la création il y a un mois. Cette école, qui devrait être installée fin 2018, permettra au Sénégal et à nos partenaires régionaux de renforcer leurs capacités en cyber sécurité, notamment dans le cadre de la lutte contre la cyber criminalité et contre le terrorisme.

b. Lutter contre les menaces informationnelles

Le deuxième enjeu, je le disais, revient à élaborer des réponses adaptées à ce nouveau défi pour notre vie démocratique que représente la propagation intentionnelle et ciblée de fausses nouvelles dans l'espace numérique.

La liberté d'information décuplée à l'âge numérique peut-être une cible pour l'arbitraire politique. Elle peut aussi être un instrument de manipulation par différents acteurs, y compris des grandes puissances. Les dernières élections, y compris en France, ont toutes été marquées par la diffusion de fausses nouvelles et par des

attaques informatiques dont le but était de troubler l'ordre public, de compromettre la sincérité du scrutin électoral, et ainsi de semer la confusion, le doute et la discorde. C'est une atteinte à la souveraineté même des Etats visés, qui profite de la passivité des plateformes face à ce phénomène inacceptable, une passivité qui, je veux le dire clairement, confine à l'irresponsabilité.

Animé par une vision cynique de l'espace numérique, ceux qui se livrent à ces manœuvres tentent de retourner contre nos démocraties les principes même qui les fondent - l'ouverture, la liberté d'information et de communication - pour en faire des instruments d'ingérence et de déstabilisation. Nous vivons un nouvel âge de la propagande. La désinformation n'est pas un phénomène nouveau bien sûr, mais la révolution numérique et ses incidences sur la manière dont l'opinion publique s'informe, et tout particulièrement notre jeunesse, lui confèrent une portée sans précédent. Il y a là une menace disruptive pour notre démocratie elle-même dont nous n'avons pas encore pris toute la mesure. La réponse à ces ingérences passe autant par l'action des pouvoirs publics, la responsabilité des entreprises que la vigilance de la société civile et des médias.

J'organiserai prochainement un événement dédié à ces questions afin de dégager des pistes concrètes de travail avec l'ensemble des acteurs concernés et afin de réfléchir aux initiatives internationales que nous pourrions prendre.

c. Lutte contre l'utilisation d'internet à des fins terroristes et criminelles

Le troisième enjeu de sécurité, c'est l'extension de la lutte contre le terrorisme dans l'espace numérique. Un des aspects clés concerne la diffusion des contenus terroristes en ligne et l'utilisation de l'internet à des fins de radicalisation, de recrutement, d'encouragement ou d'incitation. Ce problème d'ampleur mondiale appelle des solutions innovantes au niveau international.

La France considère, avec ses partenaires européens, que les entreprises du secteur numérique doivent assumer leurs responsabilités dans la lutte contre le terrorisme et la criminalité en ligne.

Le président de la République et la Première ministre britannique, Theresa May, ont lancé en juin 2017 un plan d'action conjoint pour lutter contre l'emploi d'internet à des fins terroristes. Dans ce cadre, il est demandé aux entreprises concernées d'agir en priorité dans trois domaines :

- premièrement, le retrait des contenus terroristes dans les une à deux heures suivant leur publication ;
- deuxièmement, la lutte contre l'enfermement algorithmique ;
- troisièmement, le soutien aux entreprises de taille plus modeste pour les aider à détecter ces contenus et à prévenir leur réapparition.

Dans ce domaine, l'efficacité de notre action suppose de faire preuve d'innovation diplomatique. La France entend donc agir avec les grands acteurs de l'internet (Facebook, Microsoft, Twitter et YouTube notamment) puisque ce sont leurs plateformes qui servent de support à ce champ de bataille d'un genre nouveau. C'est de cette manière que nous pourrons lutter efficacement contre la propagande, le

recrutement, la planification opérationnelle à des fins terroristes, ainsi que la dissémination en ligne des discours et des images de haine.

Afin d'obtenir des avancées concrètes, le président de la République et le Premier ministre ont chargé David Martinon, Ambassadeur pour le numérique, de conduire un dialogue direct avec les grandes plateformes numériques. La France mènera ce dialogue en lien avec le Royaume-Uni et l'Allemagne.

d. Les conditions de la cybersécurité collective

Le quatrième et dernier enjeu, le plus structurant, c'est celui de la sécurité internationale dans l'espace numérique. Pour être garantie, elle demande là aussi un effort de régulation, adossée à trois principes : la prévention, la coopération, et la stabilité.

Pour faire émerger ce cadre de cybersécurité collective, la position de la France est claire : nous devons nous appuyer sur les équilibres définis par le droit international, et notamment la Charte des Nations Unies, dans son intégralité. De ce principe simple découle un certain nombre de règles, que chaque Etat est tenu de respecter.

Je pense, par exemple, à l'obligation de régler ses différends internationaux par des moyens pacifiques. Bien entendu, cela ne remet aucunement en cause le droit de chaque Etat à prendre des contre-mesures en réponse à un fait internationalement illicite commis à son encontre, réponse dont l'unique objectif doit être de mettre un terme à celui-ci, conformément à ses obligations en droit international.

Ces contre-mesures devront être strictement pacifiques, nécessaires et proportionnées à l'objectif poursuivi. Dans certains cas, de telles mesures pourront être prises de manière conjointe ou coordonnée avec certains de nos partenaires et alliés. L'Union européenne s'est ainsi dotée récemment d'une *cyber toolbox* qui permet de répondre de façon conjointe aux activités malveillantes dans le cyberespace.

Je pense également à la capacité, de chaque Etat, dans les cas où une attaque informatique serait constitutive d'une menace contre la paix et la sécurité internationales, de saisir le Conseil de sécurité des Nations Unies, au titre des chapitres VI ou VII, de la Charte des Nations Unies.

De plus, sous réserve d'une appréciation des circonstances d'espèce, une attaque informatique majeure pourrait constituer une agression armée au sens de l'article 51 de la Charte des Nations Unies et ouvrirait dès lors la possibilité d'invoquer le droit de légitime défense, dans l'attente d'une décision du Conseil de sécurité. Si elle était dirigée contre un membre de l'OTAN, elle pourrait de même donner lieu à l'invocation et à la pleine application de la clause de solidarité de l'article 5 du traité de l'Atlantique-Nord.

Enfin, je rappelle également l'applicabilité, dans le cyberespace, du droit international humanitaire, c'est-à-dire le droit de la guerre, dont les grands principes sont la nécessité, la proportionnalité, la distinction et l'humanité.

A ces règles directement issues du droit international, s'ajoutent ce que l'on appelle des normes de comportement responsable applicables à la conduite des Etats dans le cyberespace. Celles-ci ont été agréées volontairement, d'abord dans le cadre des groupes d'experts gouvernementaux de l'ONU, puis endossées par l'Assemblée générale des Nations Unies. Il revient désormais à chaque Etat de mettre en œuvre ces recommandations et de respecter ces normes.

Afin d'accroître la confiance au niveau global, et de limiter la prolifération des risques et des menaces dans l'environnement numérique, la France poursuivra un dialogue coopératif avec l'ensemble des partenaires internationaux qui y sont prêts, publics et privés, sur le plan bilatéral et multilatéral.

Nous encouragerons la mise en œuvre de mesures de confiance, comme a déjà pu le faire l'OSCE en créant un réseau de points de contact d'urgence, activable en cas de crise cyber. Et parce que les conflits dans le cyberspace mêlent de plus en plus des acteurs publics et privés, parce que de plus en plus souvent des opérations étatiques se dissimulent derrière des actes de cybercriminalité, la France continuera, en étroite concertation avec ses partenaires, d'apporter une réponse judiciaire aux attaques cyber. Elle soutient pour cela l'universalisation de la Convention de Budapest sur la lutte contre la cybercriminalité, seul instrument véritablement efficace de coordination internationale des services d'enquête.

Enfin, l'irruption du numérique comme outil et espace de confrontation confère au secteur privé, et notamment à un certain nombre d'acteurs privés systémiques, un rôle et des responsabilités inédites dans la préservation de la paix et de la sécurité internationales. Il faut donc que les Etats engagent entre eux, mais aussi avec le secteur privé et le monde de la recherche, de nouveaux travaux afin de définir des formes de régulation adaptées à l'évolution du monde numérique et permettant de renforcer la stabilité, la coopération et la confiance de tous les acteurs dans le cyberespace. Je crois que nous devons ici plus particulièrement agir et innover dans trois directions :

- d'abord, renforcer la sécurité des produits et des services numériques afin de s'assurer qu'ils ne puissent pas être détournés de leur usage initial pour conduire des attaques informatiques ;
- ensuite, lutter contre la prolifération et la commercialisation d'outils, de techniques ou de logiciels informatiques malveillants dans le cyberespace, notamment via le contrôle des exportations des biens cyber à double usage;
- En outre, interdire strictement les actions offensives du secteur privé dans le cyberespace. Je pense notamment à la pratique du hackback qui consiste, pour un acteur privé, à s'arroger un droit à mener une contre-attaque dans le cyberespace. Des dérogations au monopole étatique de la contrainte légitime, y compris dans le cyberespace, ne peuvent que susciter une instabilité supplémentaire contre laquelle nous devons nous prémunir.
- Enfin, la prise en compte de l'importance du secteur privé implique d'élaborer de nouvelles relations entre les entreprises et l'Etat. Il est donc nécessaire de

travailler au développement de forum où ce dialogue pourra se dérouler. Je suis convaincu que pour produire de nouvelles normes, l'Etat doit prendre l'habitude de développer ce genre d'instruments. J'entends donc agir en ce sens pour ce qui concerne les enjeux internationaux du numérique.

Vous voyez combien l'espace numérique, pour être régulé, demande une action diplomatique professionnelle. C'est un enjeu que mon ministère prend d'ores et déjà en compte et pour lequel il nous faut passer à la vitesse supérieure. Au lendemain de la seconde guerre mondiale, notre diplomatie a répondu à la nouvelle donne stratégique que représentait l'énergie nucléaire par la formation de ses diplomates à ces questions. Nous devons désormais fournir un effort analogue pour le numérique, avec l'objectif de former, sur les plans technique, politique et stratégique, une véritable filière de diplomates cyber, en lien avec les autres administrations de l'Etat, avec les entreprises, les centres de recherche et avec nos partenaires internationaux. Le quai d'Orsay y prendra toute sa part. De même qu'il est un pôle d'excellence reconnu pour les questions stratégiques internationales, il devra j'en suis convaincu, passer du stade actuel, celui de la formation d'agents spécialisés sur les questions de cybersécurité, à la mise en place de structures spécifiquement dédiées aux enjeux diplomatiques liés au numérique.

En parallèle, nous devons également nous doter des moyens nécessaires au développement d'une pensée stratégique française sur la cybersécurité. De nombreux chercheurs et chercheuses réputés travaillent déjà sur ces questions. Certains sont présents aujourd'hui, je pense à la Chaire Castex de Cyberstratégie ou encore au réseau interdisciplinaire d'experts AMNECYS, et je les salue. Cette volonté de développer une pensée stratégique s'illustre également au travers du Forum international de la Cybersécurité qui est désormais un grand rendez-vous européen et international à Lille.

Sur ce sujet d'avenir, il est impératif de continuer à se doter de compétences et de connaissances en termes de prospective, de recherche et d'expertise pluridisciplinaire. Le ministère de l'Europe et des affaires étrangères soutiendra la constitution de ce domaine à part entière de la recherche stratégique. Il doit nourrir notre action diplomatique, en lien avec le Secrétariat d'Etat au numérique.

Mesdames et Messieurs,

En commençant ce discours, j'évoquais les différentes ruptures du siècle passé et, parmi elles, je rappelais ce qu'avait représenté la conquête spatiale. Elle fut un temps l'enjeu d'une rivalité exacerbée entre les puissances avant que les adversaires d'hier ne décident de mutualiser leurs efforts. De façon analogue, le numérique est aujourd'hui la nouvelle frontière de la compétition mondiale ; le défi que nous avons à relever, c'est d'en faire également un nouvel espace de coopération. Il n'annulera pas la concurrence ; elle est légitime dans un monde ouvert où chaque acteur doit pouvoir défendre ses intérêts. Mais elle a besoin d'un cadre qui garantisse la stabilité sans laquelle il ne peut y avoir de réussite durable pour quiconque. C'est la voie que propose la France à travers sa stratégie internationale. Et c'est dans cette direction

que nous sommes résolus à agir et à convaincre nos partenaires. Merci de votre attention./.