Discours de monsieur Jean Yves Le Drian
« European Cyber Week 2022 »
Rennes – le 17 novembre 2022.

Mesdames et Messieurs,

I/ J'ai vécu 10 années d'accélération, de brutalisation de la vie internationale à laquelle nous sommes désormais confrontés au quotidien, la brutalisation numérique occupe une place qu'il faut bien qualifier d'*éminente, de symptomatique et, à bien des égards, d'emblématique*.

1/ Cette brutalisation de la vie internationale se joue, en effet, d'abord au confluent d'attitudes qui concourent à rendre notre monde moins régulé. A commencer par la remise en cause méthodique des principes et des institutions du **multilatéralisme,** et par un certain nombre de violations décomplexées des principes fondamentaux du **droit international**. Et il est clair que ***la révolution numérique participe à ce phénomène général d'affaiblissement de nos cadres de régulation internationaux***, ne serait-ce que dans la mesure où elle met au défi les règles existantes par tout ce qu'elle porte en elle de nouveau et d'inédit.

2/ La brutalisation de la vie internationale se joue aussi au confluent d'actes qui témoignent d'une désinhibition croissante de la violence - de la multiplication des **conflits** à la diffusion planétaire de **l'hyperviolence terroriste**, en passant par la banalisation des tentatives de **fait accompli**. Et il clair que *le numérique offre de **nouvelles armes** à ceux – quels qu'ils soient : groupes étatiques, organisations criminelles, mouvements terroristes ou hacktivistes – qui veulent frapper les États, les sociétés, les acteurs économiques ou même de simples citoyens.*

Vous êtes bien placés pour le savoir, puisque vous travaillez précisément à **contrer ces menaces nouvelles**, dans le champ de la **cyberdéfense** et de la **cybersécurité.**

- Ces menaces, elles sont d'autant plus redoutables qu'elles sont fondamentalement **asymétriques.** Ce qui m'est apparu le plus frappant, quand j'ai commencé à me pencher sur

ce sujet il y a dix ans, c'est **la capacité d'un adversaire à causer à peu de frais des dégâts énormes** quand on la compare aux moyens humains, matériels et financiers et aux niveaux de préparation, de logistique, de soutien requis dans la guerre conventionnelle.

- Ces menaces, elles s'intensifient à mesure que progresse la **sophistication des armes cyber**. Je pense, par exemple, aux risques nouveaux liés au développement du **quantique**, qui pourraient toucher des domaines jusque-là relativement épargnés, comme les techniques de chiffrement gouvernemental.

- Ces menaces, elles vont de pair avec la numérisation de nos propres systèmes d'armes, la numérisation des infrastructures critiques de notre pays, la numérisation de nos services publics, la numérisation de notre tissu économique, la numérisation de nos chaînes logistiques – comme nos **activités maritimes et portuaires**, ce qui me donne l'occasion de saluer l'initiative *France Cyber Maritime* qui se développe à Brest, le Cross de la cyber –, la numérisation de nos collectivités locales, et, tout simplement, la numérisation de nos vies, dans toutes leurs dimensions. **Toujours plus connectés, nous sommes – en un mot – toujours plus *exposés.***

3/ La brutalisation de notre monde se joue, enfin, au confluent de divers efforts de manipulation des opinions et, plus généralement, de travestissement de la réalité qui visent à saper la possibilité même d'un accord sur les faits, et donc la possibilité même de la diplomatie, le déni de faire devient la vérité.

- De ce point de vue, il est clair que *les réseaux sociaux , les nouveaux médias et Internet ont donné un nouvel élan aux **opérations informationnelles**,* qui sont aujourd'hui plus faciles à mettre en œuvre et plus efficaces qu'elles ne l'ont jamais été dans leur très longue histoire.

* Jamais il n'a été aussi facile de désinformer et de déstabiliser nos sociétés.

* Jamais il n'a été possible de répandre mensonges et contre-vérités aussi rapidement et aussi massivement.

- Il est également clair, par ailleurs que ***l'attribution même des attaques cyber et des ingérences informationnelles s'avère toujours extrêmement délicate.*** A la fois pour des raisons techniques et en raison du type de liens qui unissent souvent les opérateurs de l'attaque à leurs commanditaires. Cela produit également un dangereux **brouillage des faits et de la réalité,** avec lequel il nous faut composer au mieux, en apprenant à **rétablir, dans les zones grises**

des actions hybrides, la clarté dont nous avons besoin pour ne pas perdre l'initiative au profit de nos adversaires.

II/ Sans surprise, la guerre de la Russie contre l'Ukraine, qui est à ce jour l'aboutissement le plus grave de ce mouvement de brutalisation du monde *et qui vient de connaître un nouveau développement très préoccupant en Pologne,* est aussi un théâtre majeur de cette brutalisation numérique.

- Dans ce conflit, des moyens cyber auront permis de **localiser des cibles** et diriger des frappes.
- De **saboter** des infrastructures critiques.
- De **pirater** différents médias d'État.
- De collecter du **renseignement** à valeur stratégique – y compris, d'ailleurs, en source ouverte.
- Ou encore de s**'en prendre à des soutiens de l'Ukraine**, comme certains pays de l'Union européenne ou – ce qui est particulièrement indigne, même si la Russie de Poutine nous a habitué au pire – à des **ONG** portant assistance à des réfugiés ukrainiens.

1/ Si surprise il y a eu, chez certains observateurs, c'est de constater que ces attaques cyber n'avaient pas produit les effets stratégiques déterminants que nous redoutions.

- Ce qui se passera ou ce que nous apprendrons dans les mois et les années à venir conduira peut-être à revoir ce constat, bien sûr.
- Mais, à l'heure où nous parlons, **ces attaques cyber n'ont manifestement permis à aucun des belligérants d'obtenir un avantage décisif.**
- Pour autant que nous puissions en juger aujourd'hui, **elles n'ont même pas non plus pesé substantiellement sur le déroulement du conflit.**

a/ Outre les explications circonstancielles[1] avancées par les experts, outre les enseignements que nous pouvons en tirer en termes de doctrine cyber et d'intégration du cyber à la manœuvre d'ensemble, j'y vois la preuve qu'**en matière de cyber, la préparation porte ses fruits.** Car nous savons que l'armée ukrainienne a travaillé à renforcer ses capacités et ses savoir-faire cyber depuis la première atteinte militaire portée par la Russie de Poutine à son intégrité territoriale et à sa souveraineté, en 2014.
b/ J'y vois aussi la preuve qu'**en matière de cyber, la coopération et la solidarité portent leurs fruits.** Car nous savons que **le soutien apporté à la résistance ukrainienne par ses partenaires internationaux, dont la France et les Européens, s'est bien sûr manifesté jusque dans le domaine cyber.**

1

c/ J'y vois donc, en définitive, **une validation des efforts que nous avons nous-mêmes engagés** pour nous préparer à agir dans le domaine cyber, par nous-mêmes et en lien avec nos partenaires et nos alliés.

2/ Sans nécessairement parler de surprise, ce qui, pour ma part, m'interpelle et me préoccupe dans le volet cyber de la guerre en Ukraine, ce n'est pas tant le « quoi ? » que le « qui ? ». Pas tant la nature et l'intensité des attaques et contre-attaques elles-mêmes que la nature et l'engagement de ceux qui les mettent en œuvre.

a/ Vous le savez : **les belligérants ont fait appel, si j'ose dire, à toutes les *bonnes volontés numériques.***

- Si bien que les combattants de la cyberguerre qui opposent l'Ukraine à la Russie sont non seulement des **cybercombattants rattachés aux forces armées et services de sécurité de ces deux pays.**
- Mais aussi **des cybercriminels, des *hacktivistes* ou même de simples particuliers désireux de contribuer aux opérations**. Et ce dans des proportions qui semblent ne rien avoir d'anecdotique.
- Il peut s'agir de **Russes** et d'**Ukrainiens**, bien sûr. Mais aussi de **ressortissants de tout autre pays**.

b/ Si ce phénomène permet de répondre à un certain nombre de problème d'ordre tactique, il ne va pas sans poser un certain nombre de **questions d'ordre juridique** pour les personnes impliquées, comme d'ailleurs des questions de sécurité numérique et physique.

c/ Surtout, il me semble que ***l'entrée en scène de ces francs-tireurs numériques dans un conflit d'une telle ampleur n'est une bonne nouvelle pour personne***.

- Tiendront-ils compte de la **grammaire de l'escalade et de la désescalade** que maîtrisent les armées – *et en ont-ils la volonté et les moyens* ?
- Respecteront-ils le **droit international humanitaire**, qui vaut aussi dans la guerre cyber?
- Veilleront-ils à ce que la massification de leur engagement n'augmente pas le **risque de prolifération des armes cyber** sur le darkweb – *et en ont-ils la volonté et les moyens ?*

Personne ne peut le dire aujourd'hui. Et **je crains que la guerre lancée par la Russie de Poutine contre l'Ukraine n'ait ouvert une *cyber-boîte de Pandore* qui devrait tous nous inquiéter**. C'est

l'une des nombreuses raisons qui font de cette guerre non seulement u**ne guerre illégale et injustifiable**, mais aussi **une guerre irresponsable.**

III/ Au regard de ce tableau sombre, depuis 10 ans la France a fait en sorte de riposter contre la brutalisation numérique de notre monde, ce fut l'un des fils rouges de mes engagements ministériels. Parce que qu'il y allait à la fois de **notre sécurité**, de **notre souveraineté française et européenne** et de **notre capacité à peser concrètement sur le cours de la mondialisation** pour y faire valoir nos intérêts et nos valeurs.

1/ J'y ai pris ma part pour donner au cyber la place qui lui revient dans l'organisation de notre outil militaire et structurer, ici en Bretagne, un écosystème de la cyberdéfense. Un écosystème breton et français dont le rayonnement, qui va bien au-delà de nos frontières, s'incarne notamment à travers le grand succès de cette ***European Cyber Week*** qui nous rassemble ici à Rennes.

a/ Dès la préparation du *Livre blanc sur la défense et la sécurité nationale* de 2013, j'ai voulu travailler à donner à notre pays les moyens de résoudre une équation complexe : accélérer encore la numérisation de nos armées, introduire des modes de travail nouveaux autour, par exemple, du combat collaboratif, investir le champ numérique afin d'obtenir de nouveaux effets dans le renseignement comme dans la manœuvre militaire.

- Bref, offrir les **moyens les plus sophistiqués** à nos armées, avec l'appui de la DGA et de nos grands industriels de défense.
- Et dans le même temps, **bâtir des protections** afin de garantir, autant que possible, leur capacité à opérer dans ce nouvel espace en toute sécurité.

b/ Tout cela, nous l'avons traduit dans un *Plan Cyber* dont je suis venu présenter les grands axes en juin 2013, non loin d'ici, à l'École des transmissions. Ce qui a abouti à la création du Pôle d'excellence cyber en 2014, pour mener ensemble les batailles de la formation, de l'innovation et de l'action économique. Le PEC allait devenir le cœur battant de la cybersécurité et de la cyberdéfense dans notre pays.

- Cet écosystème trouvait naturellement sa place ici, en Bretagne. Il y avait déjà l'alchimie. Pour une raison objective : **la Bretagne concentrait déjà l'excellence académique** – avec ses grandes écoles et universités –, **l'excellence industrielle** – avec tous les grands acteurs du domaine, mais aussi de très nombreuses PME – **et enfin les moyens les plus avancés du**

ministère de la Défense, dont la DGA Maîtrise de l'Information, la DIRISI[2], l'École des transmissions, Saint-Cyr Coëtquidan et bien d'autres.

- En moins de dix ans, le ***Pôle d'excellence cyber*** **a permis l'émergence de plusieurs chaires, d'une école universitaire de recherche et de près de 80 thèses.**

* Il a rendu participé à nombre de projets européens.

* Il compte aujourd'hui 96 adhérents qui, au fil des années ont rejoint les 13 premiers membres industriels, parmi lesquels comptaient déjà *Thales, Airbus, Cap Gemini, Naval Group, EDF* ou encore *Sopra.*

* Et, à sa manière, il a inspiré le ***Campus cyber*** qui a récemment vu le jour à Paris.

- Je veux saluer toutes celles et tous ceux qui ont contribué à cette magnifique réussite – à commencer par **Philippe Verdier**, son premier président, et l'**Amiral Coustillière**, qui a brillamment repris le flambeau que je me réjouis de retrouver ici aujourd'hui.

Il inspire aussi le projet de campus cyber régional. Je salue le travail fait en ce domaine par le Président de la Région, Loïg Chesnais-Girard, son conseiller délégué Jérôme Tré-Hardy, et avant lui Bernard Pouliquen, ainsi que Rennes Métropole.

Une galaxie prometteuse s'est mise en place, ici à Rennes.

Cet ensemble nous permet de tenir notre rang, nous les Bretons.

Cet ensemble nous permet de tenir notre rand, nous les Français, dans le débat international.

d/ En décembre 2016, à Bruz, dans les locaux de la DGA Maîtrise de l'information, il fallait rappeler la nécessité de « repenser profondément notre manière d'aborder l'art de la guerre » du fait de « l'émergence d'un nouveau milieu, d'un champ de bataille cyber ». Et les grands **principes** qui devaient diriger notre action – **renseignement, protection et lutte offensive**, pour neutraliser les menaces mais aussi pour riposter aux attaques, voire pour frapper dans le cadre d'un affrontement conventionnel.

e/ Mes successeurs au Ministère des Armées ont ensuite poursuivi l'effort pour sécuriser les opérations menées par nos forces et les matériels qu'elles utilisent, et pour soutenir le *Pôle d'excellence cyber*. Je suis heureux de constater que **les efforts en ressources humaines** que nous avions portés ont été également poursuivis.

Il faut maintenant encore renforcer nos recrutements sur le bassin rennais. Je suis d'ailleurs ravi de devenir le Parrain de la 2e promotion des Cadettes de la Cyber !

2/ Au Quai d'Orsay, mon expérience récente m'a convaincu <u>prolonger la dimension européenne</u>

[2]Direction interarmées des réseaux d'infrastructures et des systèmes d'information

de cette réponse française à la brutalisation numérique. En suivant une triple conviction.

- La conviction que **la souveraineté européenne que nous bâtissons à 27 est le prolongement et, à vrai dire, la meilleure garantie de notre souveraineté nationale** dans un monde de rapports de forces, de jeux de puissance et de compétition à outrance.
- La conviction que, dans ce XXIe siècle fait d'autant d'opportunités que de menaces technologiques, **notre souveraineté sera *aussi* numérique et cyber, ou elle ne sera pas.**
- Et la conviction que **cette souveraineté numérique européenne doit passer par la construction de notre propre modèle numérique européen**, dans le sillage de ce que nous avons commencé à faire avec le RGPD[3] de 2016. Un **modèle de protection et de liberté**, qui montre que nous n'entendons pas nous résoudre à l'alternative entre une sorte de **far-west numérique** où tous les coups sont permis et un **autoritarisme 2.0** qui gagne du terrain dans certaines régions du monde.

Cette triple conviction, pendant cinq ans, le gouvernement français a œuvré pour la mettre en œuvre aux côtés de nos homologues européens – jusqu'à la ***Présidence française du Conseil de l'Union européenne*** du premier semestre 2022, qui a permis de faire aboutir plusieurs de chantiers majeurs.

a/ Dans le **domaine de la cyberdéfense,** nous avons organisé des **exercices** destinés à tester les capacités de réponse de l'Union européenne face à une crise cyber en janvier et en février, soit juste avant le début de l'invasion russe contre l'Ukraine.

- C'était un hasard de calendrier.
- Mais, sans évidemment rien révéler de ce qui ne peut l'être aujourd'hui, le fait est que ces exercices ont permis d'envoyer un signal de très grande fermeté.

Nous nous sommes dotés d'une boussole stratégique avec la mobilisation du COMCYBER et de l'ANSSI. **La Présidence française de l'Union européenne a aussi permis de développer des réseaux nécessaire à une meilleure coopération européenne en matière de cyberdéfense, de renforcer les capacités de cyberdéfense de l'UE et de consolider nos principes et concepts stratégiques communs**, à travers notamment l'adoption du premier livre blanc européen en matière de sécurité et de défense, et l'adoption de la **Posture Cyber de l'Union européenne**, qui précise la manière dont les orientations de la Boussole seront mises en œuvre dans le domaine cyber. C'est une priorité dans le **renforcement de la défense européenne**, qui – dans le domaine de la cyberdéfense comme dans tous les domaines – contribue au **renforcement de l'OTAN**.

[3]Règlement général sur la protection des données.

Vous l'aurez compris : **les efforts portés par l'Union européenne pour favoriser la coopération entre ses membres, mettre en place des outils communs, partager le renseignement et agir pour la sécurité numérique sont tout à fait essentiels.**

- L'idée d'un *Gallileo* cyber pour l'UE qui créerait une **infrastructure commune européenne de détection des attaques** fait son chemin.
- Et la **Commission** a très récemment publié une communication sur la cyberdéfense.

Pour moi, il est donc très clair que, sur ce sujet-là *aussi*, l**e temps de l'innocence et la naïveté européennes est bel et bien révolu !**

Il faut maintenant aller plus loin, *et plus vite*, dans le **passage de la prise de conscience à la prise de responsabilités**, par des actes. Et je sais que notre *Pôle d'excellence cyber* continuera à jouer tout son rôle dans cette dynamique.

Il faut **aller vite**, oui, pour nous préparer à faire face aux **menaces d'aujourd'hui**, mais aussi aux **menaces de demain**. Nombre de domaines de souveraineté européenne sont concernés : les transports, la santé, l'espace ou encore l'industrie. Et nous devrons faire face.

b/ Dans le **domaine normatif**, celui qui fixe les règles, c'est celui qui gagne. La PFUE a abouti à la publication de deux nouveaux règlements européens très importants. Vous le savez.

- Le **règlement sur les marchés numériques,** dit DMA, qui servira à prévenir les abus de position dominante des géants du numérique et à offrir plus de choix aux consommateurs européens.
- Et le **règlement sur les services numériques**, dit DSA, qui permettra de mieux lutter contre les contenus et produits illégaux en ligne, comme les discours de haine et les manipulations de l'information.

Les 2 directives adoptées, c'est un acte dans la marche en avant dans la référence normative au niveau européen.

c/ Et je n'oublie évidemment pas le **domaine de l'innovation**. A cet égard, je retiens notamment que la PFUE a permis de lancer **un PIEEC[4] de *cloud* souverain européen** dont nous mesurons tous, aujourd'hui, l'intérêt critique.

[4] Projet Important d'Intérêt Européen Commun

3/ Voilà, pour ainsi dire, le volet de « protection » du modèle numérique européen que nous sommes en train d'inventer. A mon sens, il est indissociable d'un volet de « projection » de notre vision du numérique.

L'enjeu, c'est d'élaborer et surtout de mettre en œuvre – *l'un ne doit évidemment pas aller sans l'autre* – de **nouveaux cadres de régulation adaptés aux menaces cyber et aux défis du numérique**. Dans ce domaine comme dans d'autres domaines stratégiques, **il nous faut des règles, de la stabilité, de la prévisibilité et de la lisibilité.**

- Nous y travaillons, avec les autres États, dans le cadre des **institutions multilatérales** des Nations unies.
- Et nous y travaillons à travers des **initiatives visant à élargir les capacités d'action du multilatéralisme,** en associant aux États les plateformes, les entreprises du secteur privé et les forces vives des sociétés civiles.

* Je pense à ***l'Appel de Paris pour la paix et la sécurité dans le cyberespace***, lancé en 2018. Il rassemble aujourd'hui environ 80 pays, 700 entreprises et de nombreuses ONG.

* Je pense à l'***Appel de Christchurch*** *contre l'utilisation d'Internet comme arme de propagande terroriste*, lancé en 2019.

* Je pense au ***Partenariat mondial sur l'intelligence artificielle***, lancé en 2020.

* Et je pense au ***Laboratoire pour la protection de l'enfance en ligne****,* lancé la semaine dernière au *Forum de Paris sur la Paix.*

A chaque fois, les Européens ont été à l'initiative. A chaque fois, nous avons réussi à produire un effet d'entrainement sur des partenaires du monde entier. De ce point de vue, force est de reconnaître que **nous avons une capacité qu'aucune autre puissance ne partage sur la scène internationale** : l'**Europe est une puissance mondiale du numérique.**

Si nous prenons acte avec le plus grand sérieux – vous l'aurez compris – de ce que **le cyber est un nouvel espace contesté et un nouvel espace de conflictualité**, nous ne perdons donc pas de vue, pour autant, qu'**Internet est également un bien commun du XXIe siècle**, dont notre intérêt est de défendre les **principes fondateurs** *avec nos partenaires.*

- Défendre le principe d'un **Internet ouvert,** contre les États autoritaires
- Défendre le principe d'un **Internet neutre**, contre un risque de fragmentation idéologique du Web et des réseaux sociaux.
- Défendre le principe d'un **Internet transparent,** face à des géants numériques qui n'ont, en

vérité, aucune légitimité pour imposer des pratiques à des milliards de consommateurs, comme ils tentent de le faire.

- Et défendre – j'y reviens – le principe d'un **Internet sûr**, contre les cyberattaques et la cybercriminalité.

Je tenais à le dire devant vous aujourd'hui, même si cela dépasse le champ de la cyberdéfense et de la cybersécurité *stricto sensu*, **afin de rappeler que l'affirmation de notre souveraineté numérique européenne n'a rien d'un *souverainisme* numérique.**

- Elle s'ordonne, bien sûr, à la **défense de notre liberté de choix et de notre liberté d'action.** C'est la définition même de la souveraineté.
- Mais elle ne constitue **nullement une forme de repli numérique.**
- Car nous n'entendons pas la construire *contre* le droit international et les règles multilatérales. Mais, au contraire, en faire **une force motrice pour adapter le droit international et les règles multilatérales aux réalités d'aujourd'hui.**

La bataille pour la souveraineté numérique européenne, dans toutes ses dimensions, y compris celle que vous portez au quotidien, est donc aussi une bataille pour *un nouvel humanisme numérique* fondé sur les principes cardinaux du droit international et sur les droits humains fondamentaux. C'est très important.

*

Mes chers amis,

Vous aurez sans doute constaté, comme moi, que la ***Revue nationale stratégique 2022*** dévoilée, il y a tout juste une semaine, par le Président de la République fait de « l'amélioration de notre **résilience cyber** » une priorité.

Vous qui êtes militaires, experts, diplomates, ingénieurs, chercheurs, entrepreneurs – *et parfois tout cela à la fois* ; vous qui êtes Bretons, Français, Européens – *et, là aussi, parfois tout cela à la fois –,* **vous jouez tous un rôle clef dans ce combat** qui engage notre avenir.

Si je tenais à être des vôtres pour clore cette nouvelle *European Cyber Week*, c'était pour vous en remercier, et pour vous inciter à poursuivre vos efforts, à tenir notre rang.

- Alors un grand merci, à chacune et à chacun d'entre vous.
- Et **au travail !**