Lettre mensuelle – Décembre 2020 – Disponible sur omc.ceis.eu

Table des matières

ANALYSES (1/2)

FAKE NEWS ET MANIPULATIONS DE L'INFORMATION, LA PROCHAINE ÉPIDÉMIE ?

Cet article est une synthèse du premier module sur trois de l'événement ***Cyberdéfense et Stratégie****, organisé entre les 15 et 17 décembre 2020 par CEIS au profit du Commandement de la cyberdéfense du ministère des Armées. Consacré à la thématique* ***« Fake news et manipulations de l'information : la démocratie en péril ? »****, cet atelier eu lieu dans un format webinar dont le replay est disponible ici.*

Les échanges ont réuni les participants suivants (par ordre alphabétique) : ***Sébastien Bombal*** *(Chef du pôle Stratégie du Commandement de la cyberdéfense),* ***Christophe Deloire*** *(Secrétaire général de Reporters sans frontières) le* ***Dr. Jacques Fradin*** *(Docteur en médecine, comportementaliste et cognitiviste à l'AFTCC),* ***Divina Frau-Miegs*** *(Professeur à l'Université Sorbonne Nouvelle – Paris III),* ***Tariq Krim*** *(Tech entrepreneur, fondateur de Jolicloud et de Netvibes),* ***David Lacombled*** *(Président de la Villa Numéris) et* ***Julien Nocetti*** *(Professeur de relations internationales à Saint-Cyr Coëtquidan et chercheur à l'IFRI).*

« *Au champ de bataille physique, se superpose maintenant un champ de bataille informationnel. Nos armées l'ont théorisé depuis longtemps, mais ses moyens ont changé et son ampleur est inédite* ».

Discours de Florence Parly, ministre des Armées, à l'occasion de la remise du rapport CAPS/IRSEM sur « *Les manipulations de l'information* » (Septembre 2018)

À l'ère du « tout numérique », l'espace informationnel ou « infosphère », repose sur un enchevêtrement d'individus produisant, relayant ou amplifiant[1] des informations, à partir notamment de plateformes d'intermédiation créées et opérées par des acteurs privés tels que Google, Facebook ou Baidu. Dans cet environnement qui favorise la diffusion de fausses informations à une vitesse six fois plus élevée que de « vraies » informations[2], les manipulations de l'information constituent un enjeu majeur pour les démocraties.

Les appellations ne manquent pas pour désigner les manipulations de l'information : *fake news*, désinformation, mésinformation, propagande, intoxication à visée politique, canular...

[1] L'amplification consiste à augmenter la portée d'une information en la partageant largement.

[2] Peter Dizikes, « Study: On Twitter, false news travels faster than true stories », *MIT News* [en ligne], 8 mars 2018.

Pour **Divina Frau-Miegs** par exemple, ce phénomène se structure aujourd'hui autour de trois dimensions : la malveillance humaine (l'intention de nuire à autrui), la malfaçon industrielle (manipuler une vraie information de sorte à porter à confusion) et l'utilisation de la technologie pour « *viraliser, tromper ou créer de la fausse militance en ligne* ». Ces dimensions rompent avec la propagande d'antan par le rôle inédit qu'elles donnent au public, qui peut désormais, grâce aux algorithmes des plateformes d'intermédiation, promouvoir certains narratifs en les amplifiant et en les viralisant.

David Lacombled insiste sur la notion de désinformation, qui consiste à tromper des individus à des fins mercantiles ou idéologiques. Les fausses informations prennent de multiples visages. Il peut s'agir :

- D'informations factuellement fausses (comme le supposé soutien du pape François à Donald Trump, annoncé par ce dernier, lors des élections présidentielles américaines de 2016) ;
- de fausses informations mêlées à des informations authentiques afin de donner une impression de véracité à l'ensemble et empêcher le lecteur de faire la part des choses. En 2017, les documents liés aux « Macron Leaks » comportait 5% de contenus erronés. Noyées dans de « vraies informations », ces fausses informations ont été dissimulées dans du vrai afin de mieux nuire au candidat Emmanuel Macron ;
- la question de la parodie se pose également : peut-elle être considérée comme de la désinformation ? Des sites à vocation commerciale, tels que le Gorafi, diffusent des informations partiellement vraies mais les détournent de façon affichée. Chaque lecteur doit pouvoir être libre de se faire sa propre interprétation.

Quant à **Tariq Krim**, il s'intéresse davantage au sujet des contenus diffusés. Il évoque notamment des « *toxicités de l'Internet* » qui prennent la forme de théories conspirationnistes, de haine en ligne ou d'intervention extérieure (de type ingérence dans les affaires intérieures d'un pays).

Quelle que soit l'approche adoptée, les manipulations de l'information ont avant tout pour objectif de tromper voire de polariser une audience cible. Utilisées à des fins politiques, elles peuvent donner lieu à ce que certains qualifient de « guerre de l'information ». Elles prennent dans ce cas la forme d'attaques informationnelles, que **Sébastien Bombal** associe à des « *actions visant à diffuser un message dans l'intention de tromper, de discréditer, de décourager ou de nuire à un adversaire* » voire de « *mobiliser des forces* » à l'encontre de ce dernier. Ce type d'attaque peut alors être comparé à une véritable « *arme de déstabilisation massive* ».

Dans cette perspective, les technologies numériques permettent d'augmenter la portée des contenus utilisés et d'atteindre ainsi de larges audiences. Quels sont les mécanismes et les conséquences de cet environnement qui favorise la prolifération – telle une épidémie – des fausses informations ? Existe-t-il des remèdes pour se prémunir contre les manipulations de l'information ?

1. Les manipulations de l'information à l'ère du « tout numérique »

Les manipulations de l'information sont un phénomène protéiforme et ancien, qui évolue en même temps que son environnement au gré des innovations technologiques. Elles prennent aujourd'hui une ampleur inédite du fait de la numérisation massive des sociétés depuis une décennie. Elles exploitent[3] notamment :

- Une technologie. À l'ère numérique, les comptes automatisés et les systèmes d'amplification sur les plateformes d'intermédiation privées constituent une innovation pour augmenter la portée de contenus ;
- des vulnérabilités sociétales, c'est-à-dire des sujets socio-politiques susceptibles de polariser des audiences ;

[3] Sébastien Bombal, Cyberdéfense et stratégie, 15 décembre 2020.

- le fonctionnement du cerveau humain, plus particulièrement les biais cognitifs, influencent la façon dont un individu perçoit une information.

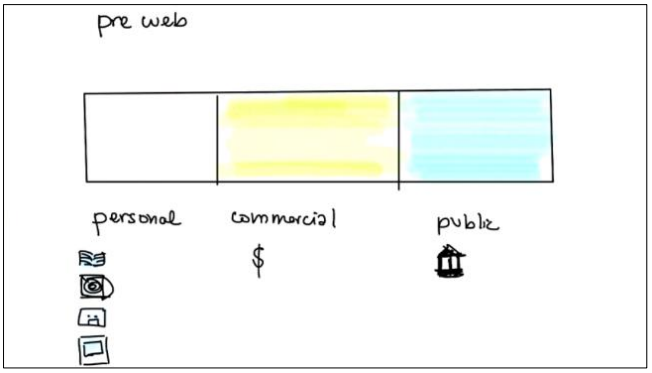
1.1. L'omniprésence des plateformes dans l'organisation des sociétés démocratiques

L'évolution de la topologie de l'infrastructure Internet et des plateformes d'intermédiation a modifié la nature des interactions en ligne. Entre les années 1970 et 1990, les échanges se limitaient à des communautés virtuelles de milliers de personnes. L'émergence des médias sociaux et des blogs à la fin des années 1990 a attiré des millions d'utilisateurs. Ces derniers ont mis fin au monopole de la production de l'information, apanage jusque-là de quelques médias, au profit d'une « communication horizontale ». Avec la possibilité de partager des informations et ses opinions, tout internaute peut désormais devenir un média et investir le débat public. Cette tendance s'est renforcée avec les plateformes d'intermédiation qui comptent aujourd'hui des milliards d'utilisateurs.

- L'émergence de l'Internet « féodal »

Depuis la fin des années 2000, l'arrivée de ce que certains surnomment l'Internet « féodal », incarné entre autres par l'iPhone et le *cloud*, a transformé le rôle des plateformes d'intermédiation. Celles-ci ont progressivement placé la monétisation au cœur de leur fonctionnement. Elles structurent aujourd'hui une grande partie de la vie privée de milliards d'utilisateurs et organisent entièrement le débat public.

Tariq Krim décline le quotidien d'un individu autour de trois espaces : un espace personnel (intimité, centres d'intérêt, relations humaines), un espace commercial (plateformes d'intermédiation privées, biens de consommation) et un espace public (vie politique, services gouvernementaux, lieux publics). La montée en puissance des plateformes a provoqué une expansion de l'espace commercial au détriment des espaces personnel et public. Pour **Christian Deloire**, l'espace public, qui était auparavant organisé par les principes édictés par les parlements, relève aujourd'hui d'intérêts privés et de la tutelle des dirigeants des plateformes.



Espaces personnel, commercial et public avant Internet – Source : Tariq Krim

- L'ère du *personal branding*

Dans un contexte où les espaces personnel et public se confondent, tout individu – dont les personnalités politiques – est un potentiel « influenceur » en quête de visibilité. C'est ainsi que sont nées de nouvelles pratiques telles que le « *hashtag activism »,* qui consiste à utiliser les hashtags des sujets les plus tendances du moment (*trending topics*), jouissant d'une portée considérable, pour viraliser des sujets politiques. Certains utilisateurs ont besoin de capter l'attention pour exister et publient pour cela régulièrement des contenus.

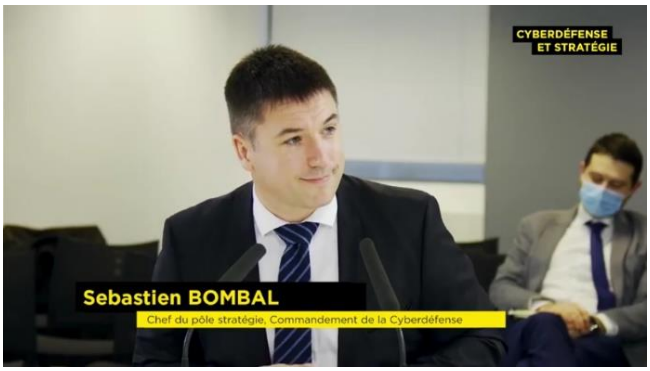
1.2. L'Internet des plateformes : un « Far West » numérique ?

L'espace commercial des plateformes présente la caractéristique de ne pas être régulé. Aux États-Unis, la section 230 (1996) les décharge de toute responsabilité quant aux contenus qui y sont diffusés. Il en est de même en France avec la loi pour la confiance dans l'économique numérique (LCEN) de 2004. Ces deux textes ont été adoptés pour encadrer l'utilisation des plateformes à une époque où celles-ci ne comptaient que des milliers voire des millions d'utilisateurs – contre des milliards de nos jours. Les législateurs n'avaient en effet pas mesuré la dimension que ces plateformes allaient avoir. Le droit en vigueur dans les deux pays ne prévoit ainsi pas leur détournement à diverses fins dont notamment celles des manipulations de l'information.

Selon **Sébastien Bombal**, l'expansion des médias sociaux dans les infosphères a ouvert une sorte de « *boîte de Pandore informationnelle* » qui exploite *a minima* les caractéristiques suivantes :

- L'émergence de nouveaux acteurs dans la production et la diffusion d'informations implique de nouvelles responsabilités pour les plateformes, les influenceurs et les relais d'information. À ce titre, **Christophe Deloire** considère que les médias sociaux ont, à l'occasion des élections américaines de 2020, fait des choix qui s'apparentent à des décisions éditoriales en annotant et en supprimant les publications de Donald Trump qu'ils ont jugées être de la désinformation. Au regard de leur rôle dans la structuration du débat public et n'étant pas des médias, la légitimité de ce type d'intervention doit faire l'objet d'un débat ;
- la compression du temps et de l'espace inhérent au milieu cyber permet à quiconque de s'affranchir des frontières. Les internautes sont en mesure d'atteindre instantanément des audiences à l'autre bout du monde et même celles jusque-là protégées des manipulations de l'information d'acteurs étrangers ;
- la démocratisation de la production de l'information a mis fin au schéma classique d'un producteur qualifié d'une information vers un récepteur. Les utilisateurs des plateformes deviennent de potentiels producteurs de contenus, alors que ce rôle était jusque-là dévolu exclusivement aux médias traditionnels ;
- les algorithmes de recommandation des plateformes promeuvent de manière ciblée certaines informations au détriment d'autres auprès d'un individu ou d'un groupe d'individus.

Accédez à l'allocution d'ouverture de Sébastien Bombal en cliquant ici :



1.3. Les nouvelles pratiques de l'économie de l'attention

L'absence de régulation de cet espace commercial favorise le *microtargeting*. L'économie de l'attention oriente le fonctionnement des plateformes d'intermédiation. Elles cherchent davantage à capter l'attention de leurs utilisateurs, afin de les exposer le plus possible à de la publicité, qu'à contrôler la nature des contenus qu'ils publient. Leurs algorithmes dits « de recommandation » créent à cet égard un système d'auto-alimentation que **Tariq Krim** qualifie « *d'inépuisable* ». Celui-ci collecte sans cesse des données visant à

mieux comprendre l'utilisateur (contenus d'intérêt, habitudes d'utilisation, état psychologique, etc.) pour personnaliser au maximum son fil d'actualité et augmenter ainsi son temps de connexion à la plateforme.

Ce ciblage organise voire enferme des individus aux opinions similaires dans des bulles dites algorithmiques ou « filtrantes » selon une logique commerciale, qui peut être détournée à des fins de manipulation. En proposant systématiquement le même type de contenus aux utilisateurs des plateformes, ces bulles renforcent les biais cognitifs des lecteurs (cf. *infra*) et les confortent dans leurs croyances et opinions. Étant peu voire pas confrontés à des opinions différentes, ces utilisateurs peuvent ainsi difficilement réviser leur jugement.

Accédez aux interventions de Tariq Krim en cliquant ici et ici :

Le premier facteur de succès et de diffusion des manipulations de l'information réside dans le fonctionnement du cerveau humain. Le **Dr. Jacques Fradin** rappelle notamment que le cerveau humain, lorsqu'il est confronté à une information, mobilise d'abord par défaut son système heuristique, lié aux émotions et aux automatismes. Le système algorithmique, qui permet à un individu de se faire une opinion, n'intervient qu'en dernier recours. En d'autres termes, un individu est naturellement davantage gouverné par ses automatismes et ses évidences sensorielles, à la base d'une partie de sa crédulité lorsqu'il est par exemple sur les réseaux sociaux, que par sa capacité de réflexion. C'est ainsi que se créent les biais cognitifs, ces distorsions dans le traitement d'informations nées de la déviation de la pensée rationnelle et logique par rapport à la réalité. Ce sont ces biais cognitifs qui expliquent pourquoi chaque individu interprète différemment une même information.

Exemples de biais cognitifs[4]

- Effet de vérité illusoire : Une information qui semble familière à un lecteur, qu'il a déjà reçue à plusieurs reprises, même fausse ou erronée, semble plus facilement véridique ;
- Effet de renforcement : Une information, en contredisant une autre, devient la preuve de la véracité de la première (exemple : pour le lecteur convaincu que le régime de Saddam Hussein possédait des armes de destruction massive, lire un texte réfutant cette information le renforcera dans ses convictions initiales) ;
- Biais de confirmation : L'individu privilégie les informations qui confortent ses positions.

Les plateformes d'intermédiation privées se sont imposées comme des acteurs majeurs de l'environnement géopolitique. En plus de transformer les rapports traditionnels de pouvoir entre les acteurs étatiques, les

[4] Voir « La désinformation : arme de distraction massive », *OMC* [en ligne], 2 septembre 2019.

acteurs non étatiques et le secteur privé[5], ces plateformes mettent à la portée de tous des outils d'influence, au premier plan desquels les manipulations de l'information.

Le développement des plateformes pose de nouveaux défis en termes de prérogatives et de souveraineté des États. Il challenge notamment la résilience des systèmes démocratiques, comme le montre leur utilisation à des fins de propagation de fausses informations et d'interférence à l'occasion d'élections nationales dans plusieurs pays occidentaux (France, Allemagne, États-Unis, Royaume-Uni, etc.).

2. La « guerre informationnelle » permanente : un enjeu de résilience démocratique

2.1. Les stratégies informationnelles : outils de politique étrangère

Dans un contexte stratégique marqué par le « retour des puissances », le champ immatériel des espaces informationnels constitue un nouveau terrain de confrontations. Le détournement de la logique commerciale des plateformes d'intermédiation à des fins géopolitiques voire idéologiques, par des acteurs étatiques et non étatiques, constitue une menace croissante. Tous ces acteurs profitent de la porosité entre les différentes infosphères pour influencer des communautés cibles en agissant sur les vulnérabilités sociétales de leur pays. Dans certains cas, l'espace informationnel s'intègre même à des stratégies globales dites « hybrides » qui mêlent la force conventionnelle à des outils cyber et de la guerre asymétrique.

Exerçant un contrôle politique sur leurs médias nationaux, la Russie et la Chine font partie des principaux États qui ont fait de leur stratégie informationnelle un outil assumé de leur politique étrangère. Selon **Julien Nocetti**, leurs manipulations de l'information s'insèrent dans des stratégies globales asymétriques et ciblent en premier lieu leurs populations respectives à des fins de cohésion nationale, avant de « s'exporter » pour influencer des audiences cibles à l'étranger (notamment en Occident). Moins coûteuses que les armes conventionnelles, ces pratiques s'inscrivent, dans ces deux pays, dans une longue tradition de propagande politique. La crise Covid-19 a constitué l'occasion d'appréhender davantage la nature de ces stratégies (cf. *infra*).

La Russie utilise le cyberespace pour influencer à bas coût et pallier ainsi sa faiblesse économique. Son objectif est d'affaiblir l'Occident en instrumentalisant ses fractures socio-politiques. Ses attaques informationnelles sont plus massives, coordonnées et offensives lorsque l'objet de la désinformation ou de la propagande concerne directement ses intérêts nationaux, comme ce fut notamment le cas pour l'Ukraine ou la Syrie. Moscou est en revanche restée relativement en retrait lors de la crise Covid-19. Le Kremlin s'appuie aussi sur ses médias internationaux RT et Sputnik pour propager ses narratifs. Difficile à contrer, leur dimension sarcastique voire quasi-humoristique à l'égard de l'Occident plaît à une large audience à l'étranger.

La Chine a adopté une stratégie différente mais qui se révèle complémentaire à celle de la Russie. Cette stratégie participe à l'affichage de sa puissance décomplexée et de son modèle de gouvernance. Lors de la crise Covid-19, Pékin a ouvertement diffusé de fausses informations avec un ton désinhibé et plus agressif, en rupture avec son *soft power* traditionnel qui consistait à véhiculer une image bienveillante d'elle-même dans le monde. Son objectif est de semer le doute auprès des opinions occidentales quant à la fiabilité et à l'efficacité de leurs dirigeants. Ciblant initialement des audiences situées sur son territoire ou dans son environnement régional, sa stratégie informationnelle s'est progressivement globalisée et mêle désormais un opportunisme tactique. Inscrite sur le long terme, elle alterne entre rhétorique conciliante et propos plus martiaux.

[5] République française, *Revue stratégique de défense et de sécurité nationale*, 2017, p. 46.

Les élections présidentielles américaines de 2020

Ce scrutin n'a jamais attiré autant d'électeurs dans l'histoire des États-Unis. Les réseaux sociaux ont joué un rôle crucial. Elles ont permis de viraliser les publications produites par les candidats des deux extrêmes de l'échiquier politique, Bernie Sanders et Donald Trump.

Ces élections ont consacré de nouveaux modèles d'utilisation des technologies et des réseaux sociaux. Considérant qu'une publication outrancière donne de la viralité et permet d'occuper le terrain médiatique, le candidat Donald Trump y a régulièrement partagé des informations infondées, telles que ses accusions du manque de fiabilité du vote par correspondance ou ses préconisations de remèdes contre la Covid-19. Cette logique du scandale vise à « créer le *buzz* ». Elle peut être opposée au modèle de Barack Obama, qui consistait à réunir un électorat autour de messages communs, ou au « compassionnel » de Joe Biden qui cherche à fédérer des électeurs autour d'idées d'apaisement.

Le scrutin a marqué un tournant dans les manipulations de l'information. En 2016, la victoire de Donald Trump s'est inscrite dans un contexte d'interférence étrangère avec notamment l'Internet Research Agency, dont les publications visaient à polariser la société américaine en exploiter les tensions socio-politiques. Les *trolls* russes avaient alors déjà introduit cette idée d'un manque de fiabilité du vote par correspondance. En comparaison, les élections de 2020 ont été l'occasion d'une « renationalisation » des manipulations de l'information avec la mouvance QAnon, qui a cherché à mobiliser l'électorat de Donald Trump autour de théories conspirationnistes en associant les élites à un réseau de satanistes pédophiles.

Enfin, ces élections américaines ont marqué un changement d'approche des plateformes. Elles ont de fait outrepassé leur rôle et pris des décisions éditoriales en supprimant certaines publications de Donald Trump qu'elles ont qualifiées de fausses informations.

Accédez à l'intervention de Julien Nocetti en cliquant ici :

2.2. Contrer les manipulations de l'information : un enjeu de stabilité pour les démocraties

Cette situation de « guerre informationnelle » permanente, qu'il s'agisse d'influence ou d'ingérence étrangère, ou plus généralement de désinformation, endommage le tissu démocratique. Elle favorise la polarisation des opinions, la montée des extrêmes, affaiblit le sens critique et appauvrit le débat public. Pour **Divina Frau-Miegs**, les sociétés occidentales sont même dans une situation « d'urgence démocratique ». Si la France peut compter sur une population relativement éduquée et a appris des expériences passées, avec les élections

présidentielles françaises de 2017 et d'autres scrutins à l'étranger, elle doit pour autant rester sur ses gardes. En effet, la France souffre toujours d'un déficit de culture numérique, médiatique et scientifique en matière de manipulations de l'information, non seulement auprès des populations les plus âgées, considérées aujourd'hui comme les plus vulnérables, mais également auprès des plus jeunes. Principaux utilisateurs des réseaux sociaux, les jeunes pourraient à terme être démunis et crédules face à des informations manipulées en ligne.

3. Rétablir un environnement informationnel fiable

3.1. Restaurer l'esprit critique

Pour le **Dr. Jacques Fradin**, le sens critique constitue « *l'une des défenses les moins mauvaises* » pour lutter contre les évidences et les fausses informations. Plus celui-ci est affaibli et plus un individu est réceptif aux tentatives de manipulation. La meilleure des défenses face à la désinformation est la connaissance de soi, du cerveau et des comportements humains, ainsi que la prise de conscience que les processus physiologiques propres aux humains peuvent les tromper. La lutte contre les manipulations de l'information passe également par la mise à nu de ce qu'il qualifie de « *fabrique du mensonge* [ou de l'illusion] » car elle permettrait, pour reprendre les termes de **Divina Frau Meigs**, de « *pré-bunker* » au lieu de « *débunker* » une information jugée peu fiable. Cette défense prévaut à celle du « *débat sans fin* » consistant à démontrer comment chaque fausse information est biaisée. En d'autres termes, « *la question apporte plus que la contre-réponse* » : apprendre à un individu à se méfier peut s'avérer plus efficace que le *fact checking*. Cette technique est d'ailleurs celle utilisée par Joe Biden lors des élections présidentielles américaines de 2020. Le candidat démocrate s'est efforcé d'interroger la source des informations de Donald Trump plutôt qu'à les contrer directement.

Accédez aux interventions du Dr. Jacques Fradin en cliquant ici et ici :

3.2. Redonner aux journalistes le rôle de « tiers de confiance »

La restructuration du secteur de l'information provoquée par l'arrivée de nouveaux acteurs, que sont entre autres les réseaux sociaux, a transformé le rôle et le modèle économique des médias traditionnels. Face à la multiplication des sources d'information en ligne, la difficulté pour le public demeure en effet de trouver celui qui lui permettra d'obtenir une information de qualité[6]. **Divina Frau-Miegs** milite pour l'introduction sur les sites d'information d'un « indice de trouvabilité » de ce type informations, ainsi que de plusieurs critères apparents tels que les niveaux de neutralité, d'indépendance et de transparence du média. L'objectif est que chaque internaute puisse se faire sa propre opinion sur la confiance qu'il accorde à un média.

[6] Le Global Disinformation Index regroupe des outils pour trouver des médias de qualité.

Accédez aux interventions de Divina Frau-Miegs en cliquant ici et ici :

L'émergence des réseaux sociaux a également fragilisé la confiance des opinions publiques envers les médias traditionnels, qui continuent toutefois d'avoir une certaine légitimité. Face à la désinformation, ces médias se sont saisis du *fact checking* pour renouer une relation de confiance avec leurs audiences, en exposant les mécanismes de fabrique des informations et notamment les fausses. Pour **Christophe Deloire**, le journaliste doit évidemment contribuer à réduire l'espace de circulation des *fake news* mais il ne lui appartient pas de « débunker » les fausses informations, au risque de se voir accusé de connivence avec un État ou un régime. En revanche, il doit s'efforcer de diffuser le plus largement des informations fiables, produites avec des méthodes professionnelles et conformes à des règles éthiques, afin de s'imposer comme un tiers de confiance. C'est d'ailleurs tout l'enjeu des démocraties aujourd'hui : outre la restauration de la confiance des citoyens envers les journalistes et les médias, s'assurer que les plateformes diffusent des informations de qualité.

Accédez à l'intervention de Christophe Deloire ici :

3.3. Des plateformes d'intermédiation plus responsables ?

Les mesures adoptées par les plateformes d'intermédiation ne sont encore pas à la hauteur des enjeux posés par les manipulations de l'information. Elles se limitent au traitement des symptômes et non des causes. Certaines, souvent dans le cadre d'une coopération avec la puissance publique, ont entrepris de réguler leurs contenus en retirant ou en supprimant les contenus considérés comme « illégaux ». Les plateformes continuent néanmoins à entretenir le flou et l'opacité sur leur fonctionnement, en pluis d'animer l'espace numérique public sans aucun contrôle démocratique.

Pour **Tariq Krim**, la solution pourrait passer par l'interdiction du *microtargeting* et donc de la monétisation de la vie privée, pratique désormais largement employée par les plateformes. Il s'agirait en fait de « casser

l'internet féodal » pour remettre en cause la toute-puissance des géants du Web, de sorte à réoxygéner le marché et à favoriser l'émergence de modèles économiques plus sains.

Une autre solution serait de refonder l'espace numérique public sur la base de principes transparents et communément admis. C'est le sens du Partenariat Information et démocratie qui compte aujourd'hui plus d'une trentaine d'États signataires (malgré l'absence notable des États-Unis). Le texte invite notamment « *les entreprises qui structurent l'espace mondial de l'information et de la communication à respecter des principes de transparence, de responsabilité et de neutralité et à assurer la compatibilité de leurs activités avec les droits de l'homme afin de promouvoir une information fiable* ».

ANALYSES (2/2)

L'intelligence artificielle pour la Défense : quel avenir pour les systèmes d'armes létaux autonomes ?

La question des systèmes d'armes létaux autonomes (SALA) est source de vifs débats, tant sur la scène politique internationale et nationale qu'au sein des opinions publiques. En juillet 2020, les députés Claude de Ganay et Fabien Gouttefarde ont présenté à l'Assemblée nationale un rapport d'information portant justement sur les SALA. Ce rapport étudie les enjeux de l'autonomisation des systèmes d'armes via des solutions basées sur l'intelligence artificielle (IA), dont les techniques ont aujourd'hui pris une place centrale dans le développement technologique et industriel de notre monde globalisé.

Pour certains, les SALA, comparés à des « robots tueurs », sont dignes de scénarios de science-fiction. D'autres sont plutôt préoccupés par les questions éthiques et juridiques qu'ils soulèvent. D'autres encore sont favorables à leur développement, considérant qu'elles répondent à la nécessité pour les forces armées de se doter de technologies efficientes dans un contexte où leurs adversaires sur le terrain sont équipés de solutions de plus en plus sophistiquées et de moins en moins scrupuleux. Si le rapport parlementaire des députés Ganay et Gouttefarde rappelle que « *à ce jour, les SALA n'existent pas* », il souligne aussi les multiples questions qu'ils soulèvent : cybersécurité, cadre juridique ou considérations éthiques, impacts opérationnels et industriels…

Alors que l'IA a aujourd'hui trouvé de nombreuses applications pour la Défense, les SALA restent un sujet particulièrement sensible. La France se distingue de certains de ses partenaires par une position pragmatique, qui prend en compte à la fois les enjeux éthiques et sociétaux, ainsi que les nécessités opérationnelles et stratégiques des Armées.

1. L'intelligence artificielle pour une défense « augmentée » ?

Identifiée comme une priorité de la défense nationale par la ministre des Armées, Florence Parly, l'intelligence artificielle (IA) est amenée à transformer toutes les activités du ministère des Armées. Plusieurs axes d'efforts prioritaires ont été définis : aide à la décision, renseignement, logistique, soutien et maintien en condition opérationnelle, combat collaboratif, robotique et cyberdéfense[7]. L'IA devrait ainsi permettre de mieux appréhender les manœuvres de l'adversaire sur le terrain, protéger les soldats, opérer des choix stratégiques

[7] « Florence Parly présente son plan en faveur de l'intelligence artificielle, axe d'innovation majeur du ministère des Armées », *ministère des Armées* [En ligne], 22 mars 2018

ou encore optimiser les flux et les ressources. Elle devrait impacter toutes les phases d'une mission allant de l'entraînement au combat sur le terrain, en passant par la planification et la conduite des opérations.

Dans le cadre de l'entraînement des personnels militaires, l'IA peut être intégrée à des programmes de simulation pour élaborer des scénarios d'engagement et les faire évoluer en fonction des réactions des personnels entrainés. Elle pourra être associée à la réalité augmentée dans le cadre de « jeux sérieux » ou d'environnements virtuels immersifs. Ces programmes permettent ainsi de maintenir le niveau de préparation opérationnelle des armées.

En outre, l'IA peut s'avérer être un outil efficace lors de la préparation des opérations grâce à la modélisation de scénarios de combat. Elle peut assister à la planification d'une opération avant le déploiement afin de tester plusieurs options et offrir aux forces armées un éventail de possibilités en matière de scénarios de déroulement d'une opération. Ces programmes peuvent aussi permettre au soldat de mettre à jour de manière continue les plans des missions, grâce à la collecte de données en temps réel sur les forces en présence, amies ou ennemies.

L'IA constitue aussi une aide précieuse pour le traitement de masses d'informations indispensables à la prise de décision[8]. Les efforts de développement de logiciels et de programmes IA dans les Armées se concentrent notamment sur des tâches de reconnaissance automatique d'objets au sein de flux de données vidéos et photos, pour permettre aux analystes de se concentrer sur des missions qui requièrent l'analyse humaine.

En matière de cybersécurité, la possibilité de traiter de grands volumes de données offerte par l'IA permet d'automatiser la détection et l'analyse d'anomalies ou de failles de sécurité en temps réel. C'est d'ailleurs sur ce segment que porte une large partie du développement de solutions commerciales (par exemple MVISION EDR et MVISION Cloud de McAfee ou bien QRadar Advisor with Watson d'IBM). Les solutions basées sur l'IA permettent ainsi d'identifier très en amont les signaux faibles ou annonciateurs d'une cybermenace. Elles sont utilisées dans le cadre d'activités de type *cyber threat intelligence* pour la prévention de fuites de données, l'analyse et la caractérisation des attaques passées, la surveillance des attaquants potentiels ou les tentatives d'attribution des attaques. L'IA permet ainsi de passer d'une sécurité « réactive » à une sécurité « proactive ».

En matière de logistique et de maintien en condition opérationnelle, des solutions basées sur l'IA alimentées par les données issues des capteurs installés sur les équipements permettent de procéder à leur gestion de manière plus efficace tout en minimisant les ressources nécessaires. Dans ce domaine, le recours à l'IA permet d'anticiper les opérations d'entretien des matériels, de commander et d'installer préventivement les pièces de rechange nécessaires. En prenant en compte les contraintes des différentes parties impliquées (utilisateurs, fabricants, sous-traitants, services des Armées) et les remontées de données des plateformes ou des systèmes de gestion des flux, les systèmes d'information permettent d'optimiser la gestion logistique et d'anticiper les opérations d'entretien des matériels et donc de commander et d'installer préventivement les pièces de rechange nécessaires.

Enfin, l'IA est bien sûr intégrée aux drones semi ou totalement autonomes qui, grâce à des systèmes multi-agents servant à gérer de manière décentralisée un système dans lequel de nombreux agents interviennent, peuvent mettre en œuvre des essaims de drones. Ces derniers sont capables de se coordonner entre eux et ont pour but de submerger les systèmes défensifs adverses ou de mener des missions de renseignement et de surveillance de manière collaborative. Les solutions basées sur l'IA peuvent également permettre aux engins robotisés d'automatiser des tâches et fonctions telles que la détection et l'identification de cibles, ou bien la cartographie d'un théâtre d'opérations.

---

[8] Alex Hillman, « No, AI and Big Data Are Not Going to Win the Next Great Power Competition », *The Defense Post* [En ligne], 18 août 2020

Parce qu'elle repose sur des algorithmes dont la principale valeur ajoutée est le traitement en quasi-temps réel de volumes gigantesques de données inexploitables tels quels par l'homme, l'IA peut rendre les personnels des Armées plus productifs, en leur permettant de se concentrer sur des tâches où les capacités humaines ont une plus-value incontestable. Ces systèmes de plus en plus connectés représentent néanmoins une porte d'entrée pour des acteurs malveillants cherchant par exemple à exfiltrer des données sensibles ou à prendre le contrôle de drones à distance. Le développement de solutions basées sur l'IA, pour la défense comme pour le secteur civil, implique donc de porter une attention particulière aux enjeux de cybersécurité. L'autre principale inquiétude suscitée par son développement concerne la place de l'humain dans ces dispositifs de plus en plus autonomes. C'est notamment tout l'enjeu des systèmes d'armes létaux autonomes.

2. Les armes automatiques, fantasme ou réalité ?

Il existe deux grands types de définitions des SALA. Les définitions extensives regroupent sous l'acronyme SALA « *l'ensemble des systèmes d'armes robotisés dotés d'une capacité létale, quel que soit leur niveau d'autonomie*[9] ». Elles incluent, outre les systèmes téléopérés, les systèmes automatiques et automatisés. Les définitions restrictives sont quant à elles centrées sur la notion d'autonomie, soit « *la capacité pour un robot de se fixer ses propres règles et de fonctionner indépendamment d'un autre agent, qu'il s'agisse d'un être humain ou d'une autre machine*[10] ». Dans leur rapport, les députés Claude de Ganay et Fabien Gouttefarde ont opté pour la définition proposée par Jean-Baptiste Jeangène Vilmer, directeur de l'Institut de recherche stratégique de l'école militaire (IRSEM), selon laquelle *« les SALA sont des systèmes d'armes capables de choisir et d'engager seuls une cible, sans intervention humaine, dans un environnement changeant*[11] ».

Si à l'heure actuelle « *la France n'envisage pas de développer des systèmes pleinement autonomes, échappant totalement au contrôle humain dans la définition et l'exécution de sa mission*[12] », elle est en revanche défavorable à une interdiction préventive de la recherche sur les armes autonomes, position adoptée par le Parlement européen. Car ces recherches devraient non seulement permettre de répondre aux questions de faisabilité technique et technologique, mais également de mieux appréhender les défis éthiques et juridiques soulevés par les SALA.

Sur le plan de la faisabilité, les inquiétudes autour de l'automatisation des systèmes d'armes létaux résident dans la capacité, ou l'incapacité, des SALA à distinguer un ennemi d'un allié et par conséquent à prendre la bonne décision et à viser un adversaire plutôt qu'un ami. Une deuxième inquiétude réside dans la sécurité des SALA, et sur la capacité de l'adversaire à les détourner et à en prendre le contrôle à distance afin de les retourner contre leur propriétaire et ses alliés. La cybersécurité des SALA est donc un enjeu majeur et devra constituer l'une des priorités des projets de recherche dans ce domaine.

En outre, seuls les pays les plus avancés technologiquement seront en mesure de développer ce type d'armement, ce qui leur donnerait un avantage militaire déterminant dans la décision de recourir à un conflit armé. Cela engendrerait une situation asymétrique qui opposerait d'un côté des machines et de l'autre des soldats.

Mais ce sont bien les enjeux éthiques et juridiques des SALA qui constituent aujourd'hui le principal frein à leur développement, et même au simple lancement de la recherche dédiée. On peut craindre par exemple que

---

[9] Claude de Ganay et Fabien Gouttefarde, « Mission d'information sur les systèmes d'armes létaux autonomes », *Assemblée nationale* [En ligne] 22 juillet 2020

[10] *Ibid*.

[11] *Ibid.*

[12] « L'Intelligence Artificielle au service de la Défense », *ministère des Armées* [En ligne], septembre 2019

la distance physique instaurée entre le soldat et sa cible par les SALA ne « désincarne » la menace, avec le double-effet de conduire le combattant à baisser son seuil d'engagement et de le rendre plus enclin à employer la force[13]. De plus, les SALA ne sont pas non plus en mesure de faire la différence entre un ordre légal ou illégal, ni donc de prendre une décision dans le contexte d'un conflit asymétrique complexe. L'IA permet d'améliorer et d'augmenter les capacités humaines mais ne remplace pas pour autant l'intervention humaine, dont les qualités comme l'empathie et l'intuition peuvent être déterminantes au moment d'engager la force.

Par ailleurs, en cas de débordement ou d'incident tels que le décès accidentel d'un civil ou le détournement d'un SALA par un acteur malveillant, la question de la responsabilité n'est pour l'heure pas évidente. Doit-il s'agir d'une responsabilité étatique ou individuelle ? À ce stade, le droit de la maîtrise des armements n'a pas défini de règles qui permettraient d'encadrer l'utilisation ou le fonctionnement des SALA. Cependant, les utilisateurs doivent en revanche respecter les normes du droit international humanitaire en vigueur.

Les inquiétudes quant au développement des SALA peuvent également s'expliquer par un flou sémantique. En effet, il est nécessaire de distinguer le système autonome du système automatisé. Le système autonome n'a pas d'opérateur humain et dispose d'une certaine indépendance avec une possibilité de choix même limités en s'adaptant à un environnement changeant. Le système automatisé réalise et répète une action préprogrammée. Ce dernier existe déjà indépendamment du développement des SALA. Un certain nombre de systèmes existants sont présentés comme « autonomes » mais relèvent en réalité de la programmation et ne sont en rien autonomes. Il existe six niveaux d'automatisation, définis par Thierry Berthier, chercheur associé au centre de recherche des écoles de Saint-Cyr (CREC), applicables aux systèmes d'armes :

- L0 : système armé pleinement téléopéré
- L1 : système armé dupliquant automatiquement l'action de l'opérateur
- L2 : système armé semi-autonome en déplacement et en détection de cibles
- L3 : système armé autonome soumis à autorisation de tir
- L4 : système armé autonome sous tutelle humaine
- L5 : système armé autonome sans tutelle humaine

Les niveaux entre L0 et L2 sont des technologies globalement bien maîtrisées par l'ensemble des puissances militaires, voire des acteurs non étatiques. Les niveaux au-delà du L2 se situent à l'état de l'art des progrès en IA et en robotique et s'appliquent à des démonstrateurs développés dans le cadre de recherches. D'importants progrès ont été réalisés jusqu'au L4, tandis que les SALA correspondraient au dernier niveau[14]. La question de l'autonomie doit être abordée sous l'angle des différents modules fonctionnels qui composent les systèmes d'armes, le développement de leur autonomie générale se faisant par paliers fonctionnels.

Puisque la capacité d'un système à évoluer dans un environnement ouvert et complexe à l'instar de l'Homme ne fait pas de lui un système intelligent ou autonome, l'application de l'IA se limite aujourd'hui à des fonctions de « soutien » des forces armées. Mais le progrès technologique et l'apparition de solutions d'autonomisation plus fiables d'une part, et de nouvelles menaces d'autre part, pourrait relancer le débat sur les SALA. L'apparition des SALA devrait être graduelle à mesure de l'apparition de nouvelles menaces. Cependant sur

[13] Romain Pinchon, « Droit international humanitaire Droit de l'Homme, Encadrement juridique des "Robots tueurs" : enjeux et perspectives », *UNOG* [En ligne].

[14] Claude de Ganay et Fabien Gouttefarde, « Mission d'information sur les systèmes d'armes létaux autonomes », *Assemblée nationale* [En ligne] 22 juillet 2020

le plan offensif, la délégation à un système autonome d'une fonction létale sera plus limitée. La position de la France, quant à elle, repose sur trois principes définis dans la stratégie du ministère des Armées sur l'IA : le respect du droit international et du droit international humanitaire, une interaction homme-machine permettant de superviser et de contrôler tout système d'arme, et la permanence de la responsabilité du commandement humain, seul responsable légitime pour définir et valider les règles de fonctionnement, d'emploi et d'engagement.

Les technologies de l'IA font l'objet d'une véritable « course à l'armement ». Aujourd'hui les États-Unis, la Chine et la Russie sont les plus actifs dans cette quête de suprématie technologique. Les progrès accomplis dans les domaines des algorithmes d'apprentissage automatique, des quantités de données disponibles, des capacités de stockage et des puissances de calcul constituent un « virage technologique » que la France ne peut se permettre de manquer, au risque de prendre le même retard stratégique et opérationnel que celui pris en matière de drones aériens. Bien qu'elle n'ait pas les moyens financiers de pays tels que les États-Unis, sa BITD, ainsi que ses capacités techniques et de recherche font de la France un compétiteur de taille.

En l'état, la réticence européenne à lancer la recherche sur les SALA pourrait conduire l'Europe à se voir dépassée sur les plans technologique, industriel et stratégique, face à des acteurs qui poursuivraient leurs efforts de recherche. De plus, le refus de développer de tels systèmes fait courir à l'Europe le risque d'un décalage avec la réalité des enjeux opérationnels et de la menace militaire[15]. Ainsi, au lieu de se prémunir contre la menace en anticipant les défis de demain, l'Europe prend le risque de se voir, dans quelques années, obligée d'agir en réaction et de développer des systèmes « dans l'urgence ».

Dans leur rapport, les députés Claude de Ganay et Fabien Gouttefarde invitent à s'appuyer sur le dialogue franco-allemand afin de parvenir à l'émergence d'une position européenne réaliste et pragmatique, permettant d'écarter tout risque d'un déclassement stratégique, technologique et industriel. Ils invitent également le gouvernement français à soutenir les engagements financiers nationaux et européens en faveur du développement de l'IA de Défense notamment dans le cadre du Fonds européen de Défense. Selon les rapporteurs, être opposés au développement de systèmes d'armes létaux pleinement autonomes ne doit conduire ni la France, ni l'Europe à se lier les mains en matière d'IA de Défense. Il faut encourager le soutien aux projets de recherche en matière de robotique et d'autonomie, au risque d'un déclassement stratégique.

[15] Patrick Bezombes, « Intelligence artificielle et robots militaires », *Areion24 News* [En ligne], 1er janvier 2020

FOCUS INNOVATION

Flint : l'IA contre les bulles d'information

Entretien avec Benoît Raphaël, Chief Robot Officer.

Présentation

Créée en 2014 par Benoît Raphaël, ancien journaliste, et Thomas Mahier, ingénieur et expert en intelligence artificielle et données, Flint est une solution de veille d'informations ayant vocation à répondre aux enjeux croissants de la surinformation et de la désinformation.

La mission

Flint est née d'un double constat : non seulement les internautes sont quotidiennement confrontés à une multitude de sources d'informations (réseaux sociaux et professionnels, blogs, flux RSS, médias en lignes, applications de journaux et magazines…), qui conduisent à la dispersion et rendent la veille d'actualité chronophage et, bien (trop) souvent, dans un contexte où les réseaux sociaux constituent la première source d'information, ces contenus sont poussés par leurs « algorithmes de recommandations » qui, sous couvert de personnalisation, enferment le lecteur dans des « bulles d'information » dangereuses.

Flint se donne donc pour mission de proposer à ses utilisateurs des informations qualifiées, diversifiées et hiérarchisées, répondant à leurs centres d'intérêt mais présentant aussi des approches ou des sujets moins habituels pour susciter leur curiosité et aiguiser leur sens critique.

Cet engagement fait de Flint une entreprise dite « à mission ». Elle compte parmi ses clients à la fois des particuliers et des professionnels, tant des organismes gouvernementaux que des PME, ETI et grands groupes, dans des secteurs aussi divers que la banque et la finance, le marketing et la communication, la transformation digitale ou encore l'édition.

La solution

Flint combine trois intelligences : artificielle, collective et individuelle.

Pour fournir à chaque lecteur un contenu personnalisé et de qualité, son algorithme d'apprentissage automatique est entraîné à la fois par ses lecteurs et par ses 400 experts thématiques, qui sont aussi ses clients.

Pour chaque lecteur, cet apprentissage comporte deux volets : l'apprentissage naturel, activé par la simple lecture d'un article proposé par sa newsletter, et un apprentissage « actif » déclenché par les réactions « j'aime/j'aime pas » sur les articles proposés dans cette même newsletter. C'est à partir de ces deux formes d'apprentissage que l'IA de Flint détermine les articles qui convienne à chaque lecture, tant en termes de thématiques que de critères qualitatifs, grâce à un algorithme combinant deux modèles :

- Un modèle social, qui repose sur l'intelligence collective et le travail des milliers d'experts qui valident la pertinence des contenus. À ce jour, ils ont observé le comportement de plus de 20 000 comptes Twitter face à des millions d'articles de tous types ;
- Un modèle sémantique, qui s'attache à comprendre le sens et la signification des mots et des articles, et créer entre eux des connexions dans le but de développer une véritable culture générale au fil des apprentissages.

Pour faire exploser les bulles d'information, l'algorithme de Flint est conçu pour :

- Surprendre le lecteur en lui envoyant, de façon aléatoire, des contenus ne correspondant pas directement à ses centres d'intérêt ou présentant des approches ou des prises de positions inhabituelles ;
- Diversifier ses sources d'information, en intégrant par exemple des contenus anglophones pouvant provenir de régions rarement couvertes par les veilles d'informations.

CALENDRIER

Forum international de la Cybersécurité (FIC) 2021 : 6, 7 et 8 avril 2021 à Lille Grand Palais)

Le Forum international de la Cybersécurité (FIC) 2021 se tiendra à Lille Grand Palais du 6 au 8 avril 2021 pour sa 13ème édition. Organisé conjointement par la Gendarmerie nationale et CEIS, avec le soutien de la Région Hauts-de-France, le FIC aura cette année pour thème : *« Pour une cybersécurité collective et collaborative ».*

La crise sanitaire majeure du COVID-19 illustre l'impérieuse nécessité de renforcer, à tous les niveaux, la coopération. Dans un monde interdépendant et interconnecté, comme dans une chaîne, le niveau de sécurité de l'ensemble correspond à celui du maillon le plus faible. Face à des risques systémiques, quelles que soient leurs origines, la seule réponse qui vaille est donc collective et collaborative. Collective, car chaque acteur est non seulement responsable de sa propre sécurité mais également de celle de chacun des autres, et donc de l'ensemble. Collaborative, car la coopération et le partage d'informations sont essentiels pour compenser l'asymétrie entre « l'attaquant » et le « défenseur ».

Après une édition 2020 qui a mis en exergue le rôle clé joué par l'Humain dans la cybersécurité, le FIC 2021 s'intéressera donc aux grands défis opérationnels, industriels, technologiques et stratégiques de la coopération. Pour les relever, le FIC s'engage à :

1. Rassembler toujours plus largement l'écosystème
2. Accélérer le développement de la filière et du marché européen de la cybersécurité en devenant sa marketplace de référence
3. Renforcer la place faite à l'innovation, en particulier en matière d'Intelligence artificielle

4. Proposer des contenus de haut niveau, toujours plus riches et diversifiés
5. Accroître encore plus son ouverture internationale et son ancrage européen
6. Adopter une approche « phygitale » permettant de combiner réalités physique et virtuelle pour un FIC « augmenté »

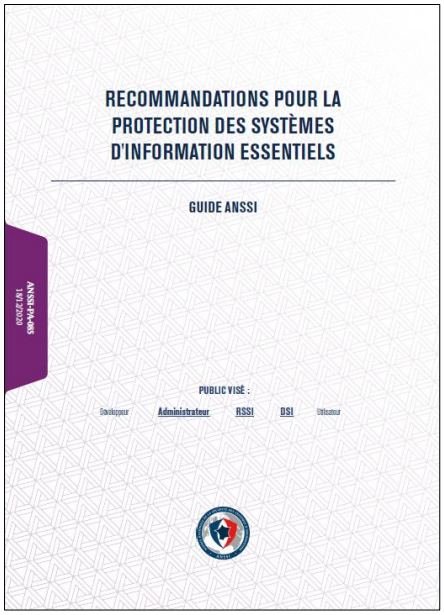
ACTUALITÉ

L'ANSSI publie un guide sur la protection des systèmes d'information essentiels

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié le 18 décembre 2020 un guide intitulé *Recommandations pour la protection des systèmes d'information essentiels*. Celui-ci est une feuille de route destinée à accompagner la mise en œuvre technique de la directive *Network and Information system Security* (NIS), adoptée par les institutions européennes en juillet 2016, qui a pour objectif d'assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne.

Les recommandations se concentrent sur les règles 7 à 16 de la directive NIS (chapitre II) qui sont spécifiquement dédiées à la protection des réseaux et des systèmes d'information (les autres règles étant consacrées à leur gouvernance, défense et résilience). Elles visent la mise en conformité, avec les règles de sécurité européennes, des systèmes d'information des opérateurs de service essentiels (OSE), des fournisseurs de service numérique (FSN) et des opérateurs d'importance vitale (OIV). Pour les autres entités, de type entreprises de services numériques (ESN) par exemple, ce guide fait office de recueil de bonnes pratiques.

Accédez aux *Recommandations pour la protection des systèmes d'information essentiels* :



La **Direction générale des relations internationales et de la stratégie (DGRIS)** propose des analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et les organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

À ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique (OMC)**, qui s'inscrit dans le contrat-cadre n°2018-02. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère des Armées
Direction générale des relations internationales et de la stratégie
60 boulevard du général Martial Valin | 75015 Paris

CEIS
Tour Montparnasse | 33 avenue du Maine | 75015 Paris
E-mail : omc@ceis.eu