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

Table des matières

ANALYSES (1/2)

CYBERDÉFENSE ET ESPACE : QUELS ENJEUX ?

Le présent article est le compte-rendu du débat en visioconférence, organisé le 29 septembre par CEIS au profit du Commandement de la cyberdéfense du ministère des Armées, portant sur le sujet « **Cyberdéfense et espace : quels enjeux ?** ». Les échanges ont réuni le **colonel (Air) Laurent Rigal** (Chef du bureau Stratégie du Commandement de l'Espace), **Sébastien Bombal** (Chef du pôle Stratégie du Commandement de la cyberdéfense) et **Michel Bosco** (Conseiller stratégique en entreprise à MAM International Consulting).

Le cyberespace et l'espace comme nouveaux champs de conflictualité analogues

L'Assemblée nationale a récemment rappelé l'avènement d'un monde multipolaire et le « retour des puissances ». Dans ce nouveau contexte stratégique, les « politiques de puissance » s'appuient sur des investissements croissants dans les technologies de pointe, ouvrant « de nouveaux champs de conflictualité tels que l'espace et le cyberespace[1] » dans lesquels les mêmes acteurs évoluent. Le budget spatial de la Chine est par exemple passé en vingt ans de 1 à 8 Mds USD/an. L'espace est désormais un domaine de confrontations au même titre que la terre, la mer, l'air et plus récemment le cyberespace.

Comme pour les autres milieux, une déclinaison cyber du milieu spatial existe et nécessite de réfléchir à l'application des problématiques cyber à l'espace. En outre, le cyberespace et le spatial sont des domaines montants et partagent un même vocable et des problématiques similaires, telles qu'être les théâtres d'une compétition stratégique entre États et soulever des besoins en ressources humaines. Ils suscitent aussi des interrogations analogues en droit international : un certain flou juridique, des réflexions sur des normes de comportement responsable et transparent…

Une déclinaison des cybermenaces à un milieu spatial en pleine évolution

Pour la France, l'espace constitue à la fois :

- Un milieu indispensable à la vie quotidienne de la population et dont l'encadrement par le droit international est régi par le traité de l'espace (1967), qui est particulièrement libéral ;
- le théâtre d'une nouvelle compétition stratégique de premier plan entre les États. Les dépenses militaires consacrées dans le monde ont quasiment doublé lors des dix dernières années ;
- un environnement dont l'accès s'est considérablement démocratisé. La réduction très significative du coût d'envoi de charges utiles a ouvert la voie à des investissements massifs d'acteurs privés, notamment dans le cadre du courant du New Space. Les États-Unis, mais également bon nombre de puissances étatiques émergentes, ont investi l'espace.

Ce cadre est favorable aux « rendez-vous de proximité », c'est-à-dire la mise en contact physique de d'objets spatiaux, qui constituent à la fois des opportunités logistiques (par exemple pour le ravitaillement des satellites) mais également des menaces nouvelles. Le nombre de satellites est aujourd'hui d'environ 2 000 et pourrait

[1] « L'évolution de la conflictualité dans le monde », *Assemblée nationale* [en ligne], 28 juillet 2020, p. 9.

être multiplié par dix dans les dix années à venir. Combinée à leur numérisation accrue, cette hausse entraîne inévitablement une augmentation de la surface d'exposition de l'espace aux cyberattaques. Le développement d'une architecture distribuée avec la logique de constellation (« système de systèmes ») est susceptible d'y ajouter de nouvelles vulnérabilités. L'enjeu cyber dans le développement du spatial nécessite d'être traité dès aujourd'hui, pour ne pas exposer les technologies spatiales à ces risques demain.

Deux objectifs majeurs de la Stratégie spatiale de défense de la France (2019)

Dans ce contexte stratégique incertain, le ministère des Armées a présenté en juillet 2019 sa Stratégie spatiale de défense (SSD) qui présente deux objectifs majeurs :

1. Le maintien de la liberté d'accès et d'action dans l'espace

À la différence du vide juridique associé au cyberespace, qui fait actuellement l'objet de débats aux Nations Unies, les activités des États en matière d'exploration et d'utilisation de l'espace extra-atmosphérique sont régies par le traité de l'espace (1967). Ce texte libéral prévoit une liberté d'action significative dans l'espace, circonscrite toutefois par un certain nombre de « lignes rouges » avec entre autres l'interdiction de militariser la Lune et de mettre sur orbite des armes de destruction massive.

Deux approches se distinguent pour faire progresser le droit international applicable à l'espace, bien que rien n'ait été encore officiellement entrepris. La première souhaite l'interdiction de toute activité militaire (position notamment de la Chine et de la Russie). La seconde appelle à l'établissement de normes de comportement responsable et promeut une transparence des activités spatiales (position de la France). À cet égard, il est nécessaire d'obtenir un consensus autour de plusieurs définitions, avec en priorité celle d'un « acte hostile » qui permettra de faire valoir la légitime défense. Il demeure que ces deux approches traduisent la nécessité de considérer la dimension militaire de l'espace[2].

2. La garantie d'une autonomie stratégique

L'autonomie stratégique suppose que la France dispose de moyens pour rallier d'autres acteurs à ses initiatives spatiales, ainsi que d'une capacité souveraine d'appréciation et d'action dans l'espace (notamment en appui à ses opérations militaires). Elle doit lui permettre d'être en mesure de répondre à la diversité des menaces émergentes, comme celles induites par les satellites, pour la protection et la défense de ses intérêts nationaux. Pour la France, la garantie de l'autonomie stratégique repose sur la diversification de sa stratégie de coopération spatiale et sur la revisite de son modèle industriel.

Le développement de capacités de surveillance spatiale

L'enjeu des données est fondamental pour la maîtrise de l'espace. La surveillance de ce milieu infini s'effectue dans la limite des capacités de détection. La caractérisation et la visualisation des objets y sont ainsi délicates. Elles supposent la collecte et le traitement d'un nombre élevé de données pour retracer l'origine de lancement d'un objet et simuler sa trajectoire. Cruciale à la prise de décision, la fiabilité des données repose sur une chaîne d'intégrité sécurisée de bout en bout.

[2] Qui ne correspond pas forcément à sa militarisation.

En parallèle de la formation aux nouveaux métiers de l'espace (tels que les opérateurs de satellite), qui relève essentiellement du Centre national d'études spatiales (CNES) et qui sera consolidée par la création d'une académie dédiée, trois objectifs de développement capacitaire sont à distinguer :

- La pérennisation des capacités d'observation, d'écoute, de radionavigation, de reconnaissance (composante spatiale optique), de télécommunications et de cartographie (système de coordonnées) ;
- la diversification et le renforcement des moyens de détection de sorte à atteindre l'autonomie dans l'appréciation spatiale (Space Situation Awareness). L'enjeu est de surveiller de manière continue l'espace et ses composantes (météorologie, objets naturels, satellites artificiels, débris, etc.) grâce à divers équipements (radars GRAVES, radiofréquence, télescopes, moyens basés sur Terre) ;
- l'adoption d'une approche de type « défense active » (ou « défense légitime »), c'est-à-dire d'être en mesure de répondre aux agressions visant les satellites d'intérêt pour la France, qu'ils soient nationaux ou européens, avec si besoin des moyens embarqués et des charges utiles dédiées.

Ces capacités d'observation et d'appréciation peuvent être décuplées par le biais de coopérations. Par exemple, la relation entre la France et l'Allemagne a contribué au développement capacitaire mutuel des deux pays en termes de radars. La coopération s'effectue également au niveau stratégique avec l'échange de données avec d'autres États, européens ou autres, notamment les Five Eyes[3]. La qualité et la fiabilité des données françaises peuvent être vérifiées en les comparant à celles des partenaires.

La coopération opérationnelle demeure également un objectif de premier plan au niveau européen. À cet égard, des réflexions franco-allemandes sont en cours pour développer un cadre dédié.

La poursuite de la sensibilisation des acteurs du spatial européen au risque cyber

Les activités dans l'espace des pays européens s'exercent majoritairement dans le cadre multilatéral de l'Union européenne. À l'échelle du continent, quatre types d'organisations spatiales contribuent à la prise en compte de la dimension « cyber » par le « spatial » : l'Agence spatiale européenne (ESA), l'Agence du GNSS[4] européen (GSA), la Commission européenne (CE) et les agences nationales. Cette diversité d'acteurs suppose des niveaux variés de sensibilisation à la cybersécurité. Bien que certains investissements aient déjà été lancés, il demeure essentiel d'intensifier les synergies entre ces acteurs.

L'ESA s'est initialement peu intéressée aux questions de sécurité. L'agence a toutefois rapidement été confronté à la « cybersécurité » dans l'espace avec, entre autres, la protection de la confidentialité de ses données et l'entretien de ses systèmes d'information embarqués. Elle a officiellement pris le tournant de la cybersécurité dans le cadre des applications militaires du programme Galileo, en se dotant d'un cyber range et d'une formation consacrée. Galileo a d'ailleurs aussi été un élément déclencheur de la prise de conscience de la CE, il y a une dizaine d'années, à ces enjeux de cybersécurité. En 2019, elle a formulé des propositions de développement pour la protection des segments sol de systèmes spatiaux (installation d'antennes, centres de contrôle sur Terre) sur les plans cinétique et cyber.

[3] Australie, Canada, États-Unis, Nouvelle-Zélande et Royaume-Uni.
[4] Global Navigation Satellite System.

New Space : l'émergence d'une filière nationale avec une approche *security by design*

La Newspace Factory (Toulouse) illustre l'émergence en France de PME et ETI qui profitent des opportunités offertes par le New Space. L'industrie spatiale étant portée par une logique de dualité civilo-militaire, la prise en compte par les industriels des enjeux de sécurité des équipements est cruciale. Le fait que les intégrateurs des systèmes spatiaux soient les mêmes que ceux des industries de défense favorise cette sécurisation. L'enjeu pour les systémiers est d'assurer une sécurité de « bout en bout » des équipements (satellites, stations de traitement de données, etc.) en prenant en compte, dès la phase de conception, les cybermenaces qui pourraient constituer de graves vulnérabilités à l'avenir.

L'adoption de cette approche security by design en matière de cybersécurité des équipements pourrait se traduire par une convention entre le ministère des Armées et les acteurs du spatial, à l'image de la convention qui unit le ministère des Armées et huit grands maîtres d'œuvre industriels signée en novembre 2019[5]. Bien qu'elle ne couvre pas l'intégralité de l'écosystème du numérique, cette convention cyber irrigue un certain nombre de sous-traitants. Elle formalise un engagement fort en faveur de la sécurisation intégrale de la chaîne de valeur de cyberdéfense, dans laquelle le CNES et d'autres acteurs spatiaux pourraient être inclus. Son efficacité repose sur l'acculturation et la sensibilisation des industries concernées au risque cyber.

La cybersécurité engage néanmoins des coûts supplémentaires pour les « petits » acteurs du New Space. Potentiels arguments de vente, ces coûts peuvent également être un frein pour les industriels. En contrepartie, l'écosystème spatial s'appuie sur quelques sociétés de niche, qui dédient des cyber ranges permettant de simuler des attaques sans endommager le système d'un satellite. L'ESA a par exemple contacté le groupe Rhea (Belgique) pour mettre en place un outil destiné à émuler des composants spatiaux (satellites, stations-sol, et.) puis les soumettre à des cyberattaques.

ANALYSES (2/2)

CYBERDÉFENSE ET CYBERESPACE À L'HORIZON 2035

*Le présent article est le compte-rendu du séminaire, organisé le 13 octobre 2020 par CEIS au profit du Commandement de la cyberdéfense, portant sur le sujet « **Cyberdéfense et cyberespace à l'horizon 2035** ». Cet atelier de travail s'est articulé autour d'interventions d'**Isabelle Chrisment** (professeure en informatique et chercheuse à l'INRIA), **Alix Desforges** (chercheuse à GEODE), **Olivier Ezratty** (auteur et consultant en nouvelles technologies et en innovation) et **Olivier Zajec** (directeur de l'Institut d'Études Stratégiques et de Défense à l'Université Lyon 3).*

En l'espace de 20 ans, Internet a profondément transformé les vies et les comportements humains. Ses domaines d'applications se sont multipliés et son utilisation a profondément bouleversé les champs socioéconomique et politique, tant au niveau national qu'international. Les technologies et les usages se multiplient et se diversifient. Ces transformations se poursuivront dans les années à venir, à l'horizon 2035 et au-delà, et impacteront tous les domaines de la société. Ainsi, le contexte

[5] Airbus, Ariane Group, Dassault Aviation, MBDA, Naval Group, Nexter, Safran et Thales.

cyber dans lequel les Armées françaises évoluent suivra cette tendance. Leurs missions comme les moyens nécessaires pour les remplir devront s'adapter.

Tous ces changements présentent à la fois des opportunités et des menaces pour les Armées. Chaque opportunité et chaque menace ne pouvant être analysée de la même manière selon qu'elle concerne ses propres forces ou celles de l'adversaire. C'est en menant cette analyse approfondie que la Défense pourra atteindre la « supériorité numérique » susceptible de conférer à ses forces un avantage décisif sur l'adversaire.

L'évolution de la cyberdéfense à l'horizon 2035 est à appréhender sous différents angles afin d'identifier les tendances structurantes du cyberespace aux niveaux géopolitique, juridique et technologique, ainsi que les conséquences opérationnelles de ces changements pour les Armées.

Vers une fragmentation du cyberespace ?

Comme dans le monde physique, la notion de souveraineté s'impose comme un principe structurant. C'est en son nom que certains pays, à l'instar de la Chine, érigent des « *donjons numériques*[6] » : l'Internet chinois, fondé sur une disjonction contrôlée par rapport à l'Internet mondial et entièrement maîtrisé par le gouvernement, fait office de modèle en matière de contrôle stratégique du domaine cyber au nom de principes tels que l'indépendance technologique, une cybersécurité robuste et la maîtrise de l'information. La Russie est souvent comparée à la Chine depuis sa tentative de mise en place de son « Internet souverain », le RuNet, lancé en novembre 2019. La mise en œuvre du RuNet, bien que partiellement déconnecté de l'Internet mondial, ne va toutefois pas aussi loin que le modèle chinois en termes de contrôle des utilisateurs. D'autres, comme les États-Unis, instaurent en réaction des « réseaux propres » (*clean network*s) en reproduisant finalement le même schéma. Le projet de *Clean Network*, c'est-à-dire d'Internet américain, accessible aux États-Unis et débarrassé de toute influence chinoise (opérateurs, infrastructures, produits, services…), « *peut-être considéré par certains analystes comme une « sinisation » de la stratégie américaine* [7] ». La notion de « réseau propre » (*clean network*) mènerait alors à celle de « propre réseau » : pour Olivier Zajec, l'un des scénarios possibles est que, tout en cherchant à conserver un Internet libre, les États-Unis se referment petit à petit sur un espace numérique national, à l'instar de la Chine et de la Russie.

Les choix de ces trois grandes puissances sont révélateurs d'une tendance au repli sur soi national dans l'espace numérique. Leur conception du cyberespace contribue ainsi à un phénomène appelé « balkanisation » d'Internet, c'est-à-dire la fragmentation d'un cyberespace universel en plusieurs espaces contrôlés par des États. Selon Alix Desforges, chercheuse chez GEODE (Géopolitique de la Datasphère), cette fragmentation comprend de nombreux risques puisqu'elle risque de « *complexifier la gouvernance du réseau et […] son fonctionnement global* », mais rendra également beaucoup plus difficile « *l'élaboration de réponse à l'échelle globale contre des cybermenaces telles que les rançongiciels* », l'utilisation de ces derniers étant en constante augmentation.[8] En outre, un cyberespace balkanisé serait plus propice au développement de la cybercriminalité, contre laquelle

[6] Propros présentés par Olivier Zajec.
[7] Propos présentés par Olivier Zajec.
[8] Propos présentés par Alix Desforges.

il sera de plus en plus difficile de lutter du fait des conceptions différentes, et donc de régulations différentes, des cyberespaces défendues par chaque État.

Nouvelles technologies, nouvelles menaces ?

Les principales tendances technologiques susceptibles de traverser le cyberespace à l'horizon 2035 comprennent :

- La multiplication des **objets connectés** ;
- L'augmentation du recours au stockage de données dans le ***cloud*** *;*
- La capacité de traitement et d'analyse de plus en plus puissante de l'**intelligence artificielle (IA)** ;
- L'arrivée de la 5G et l'explosion des performances des connexions mobiles.

De fait, ces tendances s'accompagnent de menaces. Dans ce contexte, l'application du principe de ***security by design*** devrait permettre de répondre à ces enjeux, en intégrant à chaque objet, protocole ou infrastructure des garanties de sécurité dès sa conception. La *security by design* implique également la mise en œuvre de systèmes de détection de plus en plus réactifs avant que les acteurs impliqués puissent prendre des décisions rapides en cas d'attaques avérées. Ces systèmes de détection sont basés sur des logiciels d'apprentissage automatique (*machine learning*) utilisant l'IA. Il s'agit néanmoins de rester vigilant car l'IA peut-être utiliser pour tromper les modèles appris (on parle alors d'*adversarial machine learning*). Ainsi, Isabelle Chrisment souligne que « *l'infrastructure, pour être résiliente, doit non seulement être réactive mais aussi proactive, en étant capable d'évoluer et de modifier* [en continu] *ses paramètres de configuration et son processus d'acquisition de connaissances* ».[9]

Toutefois, le nombre d'**objets connectés** continue et continuera d'augmenter, augmentant de fait la surface d'attaque sur la couche logique[10] du cyberespace. Les objets connectés grand public, souvent peu ou pas sécurisés pour des raisons de coût, présentent de nombreuses vulnérabilités et sont des portes d'entrée faciles pour de potentiels attaquants.

D'autres technologies, encore émergentes, sont également susceptibles de transformer le contexte dans lequel s'exercera la cyberdéfense à l'horizon 2035, mais leur impact reste encore incertain. On peut citer par exemple :

- Le ***edge computing***, qui permet de réduire les besoins en bande passante en proposant un traitement des données au plus près de leur source ;
- La blockchain, un système qui fait converger stockage sécurisé des données, système distribué et cryptographie ;
- La **réalité virtuelle et augmentée**, déjà expérimentée dans de nombreux domaines et en constant perfectionnement ;
- L'**impression 4D**, qui permet d'ajouter une dimension mécanique à un objet imprimé en 3D ;

[9] Propos présentés par Isabelle Chrisment.

[10] Le cyberespace est souvent considéré à travers trois couches : physique (les matériels), logique (les logiciels) et sémantique (l'information qui circule dans le cyberespace)

- L'informatique quantique, qui augmentera considérablement la puissance de calcul des ordinateurs pour la résolution de problèmes complexes.

En outre, comme le rappelle Olivier Ezratty, certaines tendances technologiques répondent à une logique purement émotionnelle difficile à anticiper, comme par exemple l'explosion des réseaux sociaux ces dernières années. De même, certains grands événements internationaux ont eu sur les usages des outils numériques un impact inattendu et imprévisible, bien que finalement particulièrement structurant. Par exemple, ce sont les attentats du 11 septembre 2001 qui ont provoqué le premier boom des outils numériques permettant de travailler à distance. Cette année, c'est la pandémie de Covid-19 qui a normalisé le télétravail et accéléré la digitalisation des outils de travail dans de nombreux secteurs et entreprises ne le pratiquant pas systématiquement.[11]

L'usage combiné de toutes ces technologies, déjà établies ou émergentes, contribue à un phénomène plus global : l'**hyperconnectivité**, qui fait elle aussi peser de nouvelles menaces pour toutes les catégories d'utilisateurs :

- Les citoyens, qui seront de plus en plus confrontés à la problématique de la protection de leurs données personnelles ;
- Les entreprises, qui sont de plus en plus victimes de cyberattaques d'ampleur (rançongiciels, vol de données, etc.) ;
- Les États, qui font face à des réels défis de souveraineté, et à des attaques de plus en plus nombreuses sur leurs infrastructures critiques, comme en France les Opérateurs d'Importance Vitale[12] (OIV).[13]

Quel droit pour le cyberespace ?

Depuis 2013, le Groupe d'experts gouvernementaux (GGE) des Nations Unis affirme que le droit international existant était applicable à l'espace numérique, que les obligations existantes sont donc suffisantes et l'adoption de nouveaux textes n'est pas forcément nécessaire. C'est en ce sens que la France a lancé en 2018 l'Appel de Paris pour la confiance et la sécurité dans le cyberespace. L'Appel de Paris propose une série de grands principes pour la régulation dans le cyberespace, dont « *l'applicabilité du droit international, un comportement responsable des États, le monopole étatique de la violence légitime et la reconnaissance des responsabilités spécifiques des acteurs privés, notamment en matière de prévention des failles de sécurité et de renoncement à certaines pratiques pouvant porter atteinte à la stabilité du cyberespace* ».

La France se positionne clairement en faveur de l'applicabilité du droit international dans le cyberespace, comme précisé dans la Stratégie nationale de la cyberdéfense, dans laquelle la France affirme sa position « *en faveur de la reconnaissance claire et univoque de la licéité des moyens de réponse à une cyberattaque, qu'ils impliquent un recours à la force (légitime défense) ou non (contre-mesures, mesures de rétorsion, etc.), et de l'applicabilité du droit international*

[11] Propos présentés par Olivier Ezratty.

[12] Un OIV est une organisation identifiée par l'État comme ayant des activités indispensables à la survie de la nation ou dangereuses pour la population

[13] Propos présentés par Isabelle Chrisment.

humanitaire aux cyberopérations conduites dans le cadre de conflits armés ». Cette position est partagée par de nombreux pays, dont la Chine ou de la Russie, qui militent malgré tout pour l'établissement de réglementations nouvelles spécifiques au cyberespace. Cette divergence majeure a donné lieu en 2018 à une scission au sein des Nations Unies, qui ralentit aujourd'hui les discussions : en parallèle des travaux portés par le GGE, à l'origine des négociations sur la régulation dans le cyberespace, la création d'un groupe de travail à composition non limitée, ou *Open-Ended Working Group* (OEWG), portée par la Russie, a été votée, multipliant ainsi les cadres de négociations et les visions en matière de régulation du cyberespace.

Quelles conséquences opérationnelles pour les Armées ?

L'hyperconnectivité aura des conséquences importantes sur les opérations militaires. Elle augmentera considérablement **la taille du champ de bataille numérique** (extension des trois couches, physique, logique et sémantique) et multiplieront la diversité des environnements technologiques. La capacité d'adaptation des Armées devra suivre.

En outre, l'hyperconnectivité provoquera la prolifération des **données**, civiles et militaires, déjà abondantes. Les données militaires sont par nature sensibles et leur protection devra rester une priorité absolue. Cela pose la question de la mise en place et en œuvre d'un *cloud* souverain dédié aux données militaires. De plus, ces données devront être traitées, ce qui impliquera l'utilisation d'outils performants, capable de traiter et d'analyser de gros volumes de données (*big data*). C'est là que l'utilisation de solutions basées sur de l'IA (*machine learning*, *deep learning*) trouve son sens pour des usages tels que la planification et la conduite d'opération, les flux logistiques, la maintenance prédictive, la gestion des ressources humaines, etc.

Adaptée à un usage militaire, la **5G** est également porteuse de promesses tout en renforçant l'hyperconnectivité. Avec une augmentation de débit (multiplication par 10 par rapport à la 4G) et une diminution de la latence (division par 10), elle pourrait permettre, dans le civil comme dans les Armées, de développer des usages tels que les véhicules autonomes, les *smart cities*, l'industrie, la chirurgie à distance, etc.[14]

[14] Propos présentés par Isabelle Chrisment.

FOCUS INNOVATION

BUSTER.AI : NOUVELLE ARME DE LUTTE CONTRE LA DÉSINFORMATION

Entretien avec Julien Mardas, CEO et cofondateur de Buster.AI.

Présentation

Buster.AI est une jeune entreprise innovante de la Deep Tech française, cofondée à Paris en 2019 par Aurélien Cluzeau et Julien Mardas.

Forts de leurs expériences dans le domaine de l'intelligence artificielle (IA) et face à de nombreux scandales comme celui de Cambridge Analytica, ils font le constat que l'information est aujourd'hui un puissant outil de manipulation. Ils développent alors un algorithme capable de lutter contre la désinformation sur les différents canaux (médias) et formats (vidéo, texte, photo) de communication, dans le but de vérifier la véracité des contenus et ainsi lutter contre les cybermenaces liées aux *fake news* et *deep fake*.

Leur solution, souveraine et indépendante, est principalement destinée aux agences de presse, médias, marchés financiers et réseaux sociaux – Buster.AI travaille par exemple avec TF1[15] sur un outil de *fact checking* –, mais s'adresse aussi au monde de la finance et aux instances gouvernementales.

La solution

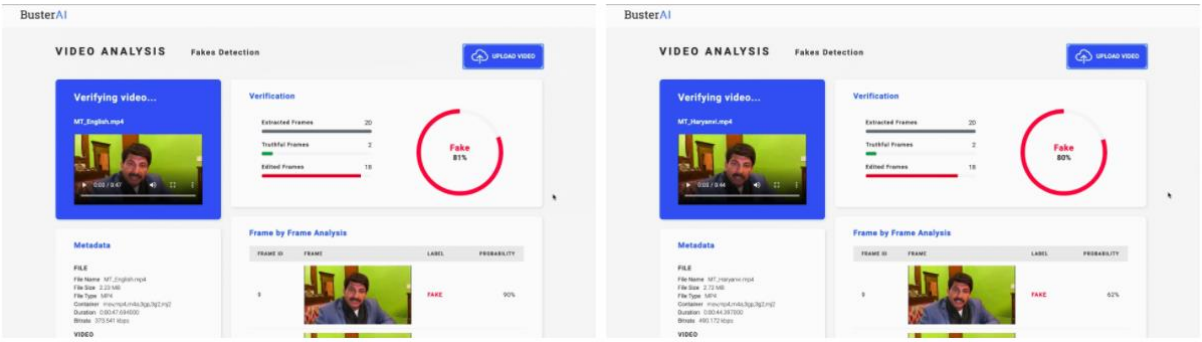
La solution, développée à partir de standards open source, se présente sous la forme d'une API intégrée à une application Web et à un plug-in pour navigateur. Via une approche holistique et journalistique, Buster.AI appréhende la fausse information comme un virus et soumet, pour chaque contenu, une analyse détaillée permettant d'expliquer les décisions de ses algorithmes d'IA en trouvant les sources officielles qui supportent ou s'opposent au contenu.

Pour le grand public, la solution a pour objectif de protéger les profils utilisateurs des *fake news* présentes sur les réseaux sociaux et les mettre en confiance sur les contenus qu'ils diffusent à leur propre communauté. Elle propose plusieurs versions selon le nombre de sources d'information et d'analyses couvertes. Pour les RSSI et les DSI, elle se présente sous la forme d'un tableau de bord qui les accompagne dans la maîtrise des risques d'atteinte à l'image de leur marque et aux tentatives de manipulation des salariés en entreprise.

[15] Buster.AI est incubée par TF1 dans le cadre du Media Lab de Station F.

Quel qu'en soit l'usage, l'objectif de Buster.AI n'est pas de prendre la décision à la place de ses clients mais de les aider à aller plus loin dans le décryptage de l'information en répondant par exemple aux questions suivantes : quelles sont les véritables intentions derrière cette communication ? La vidéo est-elle vraie mais le texte falsifié ? etc…

L'exemple des élections législatives indiennes de février 2020[16] est particulièrement frappant et met en lumière l'approche multimodale de la solution (« mélanger l'image, la vidéo, le texte et remettre les choses en corrélation pour aider à une décision finale »[17]). L'étude de vidéos de campagne diffusées par l'un des partis politiques impliqués par les algorithmes de Buster.AI a révélé que seules 2 images sur 18 pouvaient être considérées comme « vraies ».



Interface Buster.AI d'analyse des vidéos du candidat Manoj Tiwari

Les technologies

Les algorithmes de Buster.AI analysent des informations en temps réel et interviennent là où le traitement humain ne suffit plus, quantitativement et qualitativement, à détecter les manipulations. La solution se positionne comme un soutien à toute forme d'analyse et de décryptage des contenus, grâce à des outils capables d'empêcher que la désinformation ne surpasse l'information.

Pour se faire, la jeune pousse utilise des outils et des technologies différents :

- Le langage de programmation Python pour ses algorithmes ;
- Les frameworks de Deep Learning PyTorch (principalement développé par Facebook AI Research – FAIR) ou TensorFlow (mis en place par Google Brain) ;
- Des solutions Cloud ou des serveurs dédiés pour tout ce qui est relatif au Big Data (données non critiques).

Par ailleurs, la société s'assure que les modèles de Machine Learning puissent s'adapter à des volumes de données significatifs et pour un nombre important de requêtes.

[16] https://medium.com/buster-ai/deepfake-videos-to-enter-politics-3a42a90c79c2
[17] Définition de l'approche multimodale donnée par Julien Mardas durant l'entretien.

Enfin, afin de répondre aux nombreux défis technologiques, elle travaille en étroite coopération avec des centres de recherche tels que l'INRIA et participe à des challenges, dont le CLEF[18] qu'elle a récemment gagné.

Perspectives

Incubés par ESSEC Ventures, et plus spécifiquement au sein du programme Media House[19], Buster.AI a déjà réalisé un premier tour de table auprès de business angels, a remporté le Challenge MINDS des agences de presse mondiales et fait partie des 100 start-up où investir en 2020 selon *Challenges*[20]. Son ambition : devenir l'antivirus de l'information.

L'entreprise cherche aujourd'hui à s'étendre sur le marché B2C via son application mobile et le plug-in et à développer ses liens avec les agences gouvernementales. Elle va également se concentrer sur les agences de presse, les grands médias ainsi que les directions communication des grands comptes, principalement dans le secteur des marchés financiers.

CALENDRIER

Présidentielle 2022 J-500 – Liberté ? Egalité ? Fake news ! (09/12/2020)

La villa numeris organise le 9 décembre 2020 une visioconférence portant sur l'ingérence électorale dans le cadre des élections présidentielles françaises de 2022. Cet évènement rassemblera des acteurs de la vie politique et des spécialistes de la lutte contre la manipulation de l'information. Ci-dessous, la présentation de la visioconférence :

Les questions qui font débats : Les démocrates ont un train de retard. Les puissances étrangères qui ont intérêt à perturber l'élection présidentielle de 2022 sont déjà à la manoeuvre. Au lendemain de l'élection américaine, quels enseignements pouvons-nous tirer de la campagne US ? Comment se sont comportés les réseaux sociaux ? Sommes-nous vraiment sûr de la sincérité du scrutin ?A plus d'un an de l'élection présidentielle française, les leçons du scrutin et des manipulations de 2017 ont-elles été tirées ? Quels enseignements des crises récentes, covid-19 et gilets jaunes ? Comment les institutions et les médias se prémuniront-ils des attaques et des entreprises de déstabilisation ? Les professionnels de la presse sont-ils suffisamment organisés et outillés ? Comment les réseaux sociaux s'organisent-ils ? Est-il encore temps de renforcer nos défenses ? Si oui, comment ?

Inscrivez-vous en cliquant ici.

[18] https://www.linkedin.com/feed/update/urn:li:activity:6727919580825571329

[19] Media House est le fruit d'un partenariat entre ESSEC Ventures, la Chaire Média & Digital de l'ESSEC et Media Maker, soutenu par le ministère de la Communication et de la Culture.

[20] https://www.challenges.fr/classements/start-up/2020/

ACTUALITÉ

L'ENISA publie son rapport Threat Landscape 2020

L'Agence de l'Union européenne pour la cybersécurité (ENISA), avec le soutien de la Commission européenne, a publié son huitième rapport ENISA Threat Landscape (ETL). Contribuant à la réalisation des objectifs formulés par la stratégie cyber de l'Union européenne, ces rapports annuels soulignent l'importance d'analyser les menaces et d'identifier les tendances émergentes en matière de cybersécurité. Cette année, le rapport ETL s'intéresse à la transformation numérique suscitée par la crise Covid-19, qui a permis à de nombreux cybercriminels d'améliorer leurs capacités. Il est une compilation de vingt-deux rapports qui identifient et évaluent les principales cybermenaces, entre janvier 2019 et avril 2020, selon plusieurs domaines et sous-domaines : stratégique (incidents, recherche et innovation, tendances), technique (CTI) et menaces (malware, phishing, déni de service, ransomware, botnet, cryptojacking, etc.).

Retrouver les différents rapport ici.

La **Direction générale des relations internationales et de la stratégie (DGRIS)** propose les 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 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 – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com