Lettre mensuelle – **Avril 2021 – Disponible sur omc.ceis.eu**

Table des matières

ANALYSES (1/2)

ATTAQUES CYBER-CINETIQUES : VERS UNE EVOLUTION DE L'USAGE DE L'ARME CYBER ?

L'année 2008 a été témoin de la première action de piratage ayant provoqué de manière certaine des dégats humains : un adolescent polonais a provoqué le déraillement d'un tram et blessé 12 personnes, après avoir adapté une télécommande de téléviseur pour en piloter les aiguillages dans la ville de Lodz. Ce type d'attaque est qualifié de "cyber-cinétique" car elle peut affecter physiquement des biens ou des personnes.

En 2012, le Secrétaire américain à la Défense Leon Panetta mettait en garde contre le risque pour les Etats-Unis d'un possible "*cyber Pearl Harbor*", consacrant le potentiel destructeur de ce type d'attaques informatiques. Une remarque alarmiste qui visait à une prise de conscience d'un scénario alors considéré comme crédible Une décennie plus tard, le risque d'occurrence qu'un tel scénario se produise semble-t-il toujours envisageable ?

1. Une frontière de plus en plus floue entre monde physique et monde numérique

Les dernières décennies ont vu le développement de systèmes informatiques contrôlant des mécanismes physiques. On parle d'informatique embarquée, voire de systèmes cyber-physiques (CPS) lorsque des éléments informatiques distincts, mais connectés en réseau, collaborent pour le contrôle et la commande d'entités physiques. Aujourd'hui, les CPS sont de plus en plus interconnectés physiquement au réseau Internet, avec plus ou moins de mesures de cloisonnement les protégeant. Cette interconnexion sert plusieurs objectifs : surveillance et maintenance de ces systèmes d'abord, mais également capitalisation sur les données qu'ils génèrent, à l'aide de moyens d'analyse de plus en plus déportés dans des *clouds*. Elle permet également diverses applications telles que le *smart grid*, la production intelligente (industrie 4.0), les véhicules autonomes et les systèmes d'armement.

Les machines ne sont néanmoins pas les seules à devenir de plus en plus dépendantes au numérique : cette tendance concerne aussi les hommes et les organisations. Du développement de l'Internet à haut débit, qui a connecté les foyers à partir des années 1990, au smartphone qui aujourd'hui ne quitte plus les individus, la vie sociale et professionnelle a été bouleversée et ne peut plus se concevoir sans intermédiaire numérique.

Cette fusion du "monde numérique" et du "monde physique" implique que les actions dans le premier ont des conséquences dans le second. C'est naturellement aussi le cas des cyberattaques qui peuvent, dans certains cas, provoquer des dégâts matériels, voire avoir des conséquences sur l'intégrité physique des individus. On peut notamment citer :

- Les attaques ciblant des CPS, dont le piratage peut provoquer des dommages par action ou inaction d'un système. Respectivement, il pourrait s'agir par exemple pour un véhicule, de provoquer un changement de trajectoire, ou de désactiver sa fonction de freinage. Une autre hypothèse formulée par des chercheurs de l'université Ben Gourion mettait en garde contre la potentialité d'une attaque sur des laboratoires de synthèse ADN, avec la création de virus biologiques à partir d'un virus informatique.
- Les attaques sur les systèmes d'information (SI) non industriels des organisations mais qui affectent ses capacités à exercer sa mission. Par exemple, lorsqu'une organisation médicale est touchée par une

attaque de type *ransomware*, les désorganisations engendrées par des atteintes aux systèmes d'informations réduisent sa capacité à prodiguer des soins aux patients.

On qualifie ces attaques ayant des origines informatiques et des effets physiques de "cyber-cinétiques".

2. Evolution de l'usage de l'arme cyber : la recherche d'effets physiques

Depuis l'exemple du tramway de Lodz, les attaques cyber-cinétique, notamment contre des infrastructures critiques et des systèmes CPS, sont devenues de plus en plus courantes. Si certaines de ces attaques sont le fait d'une cybercriminalité classique, à laquelle correspond une partie des campagnes de *ransomware* ciblant des hôpitaux, d'autres semblent bien être liées à des actions commanditées par des États. Bien que la majorité des actions cyber offensives étatiques sont avant tout axées sur l'infiltration à des fins de renseignement, les États-Unis et Israël semblent, dès 2010, avoir tenté, via le *malware* Stuxnet de provoquer des explosions au sein de centrifugeuses afin de ralentir le programme nucléaire iranien. Des attaques ciblant des infrastructures en Russie et en Iran illustrent également cette tendance à la multiplication des attaques cyber-cinétiques.

L'exemple iranien : les infrastructures critiques civiles, cibles privilégiées

Si dans la première partie de la décennie les actions cyber attribuées à l'État iranien étaient plutôt proportionnées et sans recherche de mise en danger physique, une transition semble s'être opérée dès 2017. Cette année-là, à la suite d'une cyberattaque ciblant une usine pétrochimique en Arabie saoudite, des experts de Symantec ont indiqué que les attaquants avaient cherché à provoquer une explosion que seule une erreur dans le code aurait finalement empêchée, mais qui aurait pu être source de dommages matériels, voire humains.

Dès l'année suivante, en 2018, plus d'un quart des campagnes employant le *ransomware* Samsam, attribuées au groupe iranien Gold Lowell/Boss Spider qui vise principalement des organisations aux États-Unis, ciblaient déjà le secteur de la santé. L'attaque la plus connue de ce groupe est probablement celle ayant interrompu de nombreux services essentiels de la ville d'Atlanta : la police, des transports en commun et les hôpitaux y ont fortement été affectés. Si aucune victime humaine directe n'a été rapportée, ce type d'opération représente un risque réel pour les populations civiles, par exemple pour les patients qui ne peuvent plus être pris en charge par l'hôpital ciblé, ou lorsque les services de police et de secours se trouvent désorganisés.

La même année, le groupe *Raspite,* suspecté d'être lié à l'Iran, a été accusé d'avoir cherché à compromettre des systèmes d'infrastructures électriques aux États-Unis, dans le cadre de campagnes de constitutions d'accès permettant aux attaquants de se doter d'une capacité à provoquer des coupures de courant dans les zones concernées. L'année 2020 a ensuite été témoin d'actions croisées de piratage de systèmes critiques entre l'Iran - notamment via le groupe Raspite - et des acteurs israéliens. Des attaques venant d'Iran ont ainsi touché des infrastructures israéliennes de traitement et distribution d'eau, en avril puis en décembre, et des systèmes liés au transport ferroviaire en juillet. De son côté, l'Iran a vu les infrastructures du port de Shahid Rajaee, son plus grand hub maritime, sévèrement touchées en mai par des attaques attribuées à Israël. On voit donc ainsi apparaître une gradation dans le ciblage d'infrastructures critiques par des acteurs iraniens.

L'exemple russe : les cyber-attaques au service d'une stratégie de guerre hybride

Cette volonté de provoquer des dommages physiques par le biais de cyberattaques est aussi perceptible auprès d'acteurs soupçonnés d'être liés à la Russie. En 2007, des attaques DDoS massives ont été lancées contre des sites webs du gouvernement, d'organisations financières et de médias en Estonie. Si celles-ci ont provoqué une certaine désorganisation, elles n'ont toutefois pas menacé des vies humaines.

À partir de 2014, la Russie a entrepris une stratégie de guerre hybride qui consiste en l'utilisation de capacités cyber en appui d'opérations plus conventionnelles. Dans le cadre du conflit l'opposant à l'Ukraine, le pays a par exemple été accusé d'avoir piraté les smartphones d'opérateurs de pièces d'artillerie ukrainiennes, afin de les localiser et de les détruire par des moyens conventionnels. Les attaquants, soupçonnés de liens avec la Russie, ont diffusé pour ce faire une version compromise d'une application Android qui a été téléchargée et employée par les opérateurs ukrainiens. Il s'agissait dans ce cas de cibles purement militaires.

En décembre 2015, ce sont en revanche les systèmes d'information de trois entreprises ukrainiennes de distribution d'électricité qui ont été ciblées, au cours de la première cyberattaque recensée ayant provoqué des dommages civils dans le pays. Celle-ci a causé un blackout de 1 à 6 heures pour 230 000 habitants de la ville de Kiev. Les pirates avaient alors saboté les micrologiciels des terminaux pilotables à distance de contrôle des disjoncteurs. Une seconde attaque très similaire a été détectée en décembre 2016, toujours à dans la capitale.

En 2017, la cyberattaque NotPetya a provoqué des dommages financiers dépassant les 10 milliards de dollars à l'échelle mondiale. L'attaque qui avait commencé en Ukraine, s'est propagée à de nombreuses entreprises occidentales du fait à la fois de la capacité d'auto-réplication du malware, mais aussi de sa cible initiale : le fournisseur d'un logiciel ukrainien utilisé par de nombreuses succursales d'entreprises étrangères pour leur formalités fiscales. L'utilisation d'un malware auto-répliquant, qui rend la propagation de l'attaque incontrôlable par son auteur même, suggère que ce dernier accepte, s'il ne les recherche, les dommages collatéraux que pourrait causer son opération. La numérisation exponentielle de nos sociétés hyperconnectées ne devrait qu'en augmenter le risque d'occurence. Dans le cas de NotPetya par exemple, rappelons que le ver a affecté jusqu'aux systèmes de surveillance des niveaux de radioactivité de la centrale nucléaire de Tchernobyl.

3. Vers une généralisation de l'utilisation de l'arme cyber à des fins cinétiques ?

Ces exemples semblent démontrer que certains attaquants acceptent, sinon souhaitent, que leurs opérations produisent des effets dans le monde physique. Dans certains cas, il s'agit même d'une volonté délibérée de mise en danger directe de populations civiles. Les cas iraniens et russes ne sont pas isolés. En Asie, on observe une dynamique similaire d'acteurs accusés d'être liés à la Chine qui ciblent des infrastructures critiques indiennes, notamment depuis le regain de tensions à la frontière des deux pays en 2020. La Corée du Nord est pour sa part accusée par les États-Unis et le Royaume-Uni d'être à l'origine de la cyberattaque Wannacry, qui a notamment paralysé le National Health Service britannique. Des groupes, supposément nord-coréens, s'attaqueraient ainsi depuis quelques années aux infrastructures critiques, dont des opérateurs nucléaires de la Corée du Sud. Enfin, certains pays membres de l'OTAN s'intéressent également à cette question, comme le Royaume-Uni, dont un représentant indiquait en 2018 que certains modules d'entraînement reposaient sur des scénarios de cyberattaques visant des infrastructures critiques russes.

Les opérations conventionnelles intègrent donc majoritairement désormais, et de façon croissante, une dimension numérique, qui pourrait en retour entraîner des conséquences cinétiques, avec un vrai risque

d'escalade chez les belligérants. Malgré cette perspective, nombre d'États n'hésitent plus aujourd'hui à prendre le risque d'une surenchère. Car de la même façon que le ciblage de certaines infrastructures critiques, notamment celles liées à l'énergie, est habituel dans le cadre d'un conflit armé, une cyberattaque visant directement ou ayant des répercussions sur une infrastructure critique pourrait être perçue comme un acte de guerre par le pays visé. Rappelons à ce titre que depuis 2014, l'OTAN considère qu'une cyberattaque peut déclencher l'utilisation de l'article 5 du traité fondateur et qu'elle peut donc être assimilée à une "attaque armée".

Ce constat appelle plus que jamais au renforcement des mesures de sécurité appliquées à la fois aux organisations et aux systèmes CPS les plus susceptibles d'être ciblés pour causer des dommages et/ou des victimes. Ce besoin accru de sécurité sur les CPS concerne autant l'opérateur que le constructeur. À ce titre, il pourrait être envisagé d'étendre ou de créer un statut dédié aux CPS sur le modèle de ce qui existe actuellement pour les organisations d'importance vitale, de façon à mieux garantir la sécurité de ces institutions et systèmes. Resterait à déterminer le niveau d'exigence requis en matière d'obligations de sécurité, et les mesures techniques et organisationnelles associées, et ce en prenant en compte à la fois des risques, notamment humains, et les enjeux économiques.

ANALYSES (2/2)

LA TRANSFORMATION NUMÉRIQUE FACE À SES GOULOTS D'ETRANGLEMENT

Les dernières décennies ont vu un développement fulgurant du numérique qui s'observe de diverses façons : croissance du volume total de données, plus grande connectivité des individus, informatisation des objets et leur mise en réseau…ainsi que des gains de performances des systèmes numériques (puissance de calcul, capacité de stockage, débits et latence, etc.), conditions *sine qua non* au développement des usages du numérique.

A mesure que le numérique s'impose dans nos sociétés, une dépendance s'installe à plusieurs niveaux. Dans le fonctionnement même des sociétés d'une part, car à partir du moment où le substrat numérique d'un objet intelligent est perturbé (cyberattaque, pénurie de composants), sa fonction initiale, auparavant considérée comme acquise, peut être rendue inopérante. Dans les capacités de recherche et de développement d'autre part, car celles-ci désormais intimement liées à la puissance des outils numériques.

Depuis les années 1970, ce sont les progrès en matière de puissance de calcul qui ont permis le développement des usages numériques. Ces avancées ont sensiblement été rythmées par la loi de Moore, qui prévoyait un doublement de cette puissance tous les deux ans. Cette cadence correspond en réalité davantage à la multiplication du nombre de transistors au sein des microprocesseurs, cœur des traitements numériques. Mais cette progression technologique jusqu'ici ininterrompue pourrait être perturbée par les tensions croissantes sur les ressources, primaires et secondaires, ainsi que par les limites physiques, logicielles ou géographiques, qui viennent remettre en cause le développement du numérique et la pérennité même des outils existants. Faut-il pour autant déjà craindre un ralentissement des progrès technologiques numériques ?

Des limites aux capacités de calcul

Le défi de la miniaturisation des transistors

Le nombre de transistors au sein des microprocesseurs en conditionne les capacités de calcul. Leur miniaturisation, qui permet de multiplier leur nombre, reste donc la condition principale pour augmenter les capacités de calcul des processeurs, et donc par extension de tout dispositif électronique. On parle de « finesse de gravure » pour définir la taille de ces transistors, que l'on mesure aujourd'hui en nanomètres. De 10 micromètres en 1971 aux 5 nanomètres d'aujourd'hui, la réduction continue de la taille des transistors a permis une croissance considérable des capacités de calcul. Mais cette miniaturisation extrême se heurte aux perturbations quantiques : les propriétés physiques d'un même matériau changent lorsque la taille de l'objet atteint un certain seuil. Les perturbations engendrées par ce changement de propriétés influent sur le comportement attendu du semi-conducteur, et ont donc un impact négatif sur la viabilité des puces.

Pour dépasser cette limite, une solution consiste à développer des puces en trois dimensions plutôt que sur un seul plan en deux dimensions. Cette solution permet ensuite d'interconnecter des couches successives de transistors au sein d'une même puce. Si ce procédé est déjà employé pour le stockage de données, avec la mémoire flash par exemple, il présente toutefois des inconvénients dans le cas des puces : outre la multiplication du risque de défauts à la fois sur chaque couche et dans leurs interconnexions, se pose la question de la dissipation de chaleur qu'elles génèrent au sein d'un microprocesseur, d'autant plus prégnante qu'elle ne peut plus être évacuée à la surface de chaque plan.

Le « mur de la mémoire »

Connu comme le « goulot d'étranglement de von Neumann », ce "mur" correspond à la disparité grandissante entre la vitesse des microprocesseurs et leur capacité à échanger et à recevoir des données de l'extérieur. Autrement dit, les microprocesseurs calculent plus rapidement qu'il n'est possible de leur acheminer les données nécessaires pour effectuer les calculs suivants. Cette situation s'explique par les limitations actuelles en termes de bande passante, auxquelles s'ajoutent des problématiques de latence.

La solution la plus immédiate semble ici encore, bien qu'elle comporte des risques de défauts et de surchauffe (cf. infra), l'adoption d'une architecture en trois dimensions, où un plus grand nombre de transistors pourraient être empilés sur un plan parallèle au plus proche des microprocesseurs.

Des algorithmes classiques encore trop limités

La transformation numérique est ralentie par la difficulté de certains problèmes mathématiques particulièrement difficiles à traiter avec les algorithmes propres à l'informatique classique.

On peut citer notamment :

- Les problèmes d'optimisation, avec par exemple le célèbre « problème du voyageur de commerce » : la détermination, pour une liste donnée de villes, de l'itinéraire le plus court pour visiter chaque ville une seule fois, tout en conduisant au final au point de départ. La capacité de résolution efficiente de ce type de problème révolutionnerait la logistique, mais aussi les autres types de distribution (électricité, télécoms, etc.), les procédés industriels ou encore le séquençage de génomes ;
- Le *big data*, avec une efficacité de recherche dans les bases de données non structurées sans commune mesure avec les capacités actuelles ;

- La simulation de systèmes complexes, qui intéresse les domaines entre autres de l'armement, de la recherche médicale, de la finance et de la météorologie.

Dans les années 1990, plusieurs algorithmes reposant sur la physique quantique ont été proposés afin de répondre à certaines de ces problématiques. Ainsi, l'informatique quantique promet des améliorations fulgurantes de nos capacités à traiter ces problèmes mathématiques.

La question de la résilience de la chaîne d'approvisionnement

Au-delà de la seule question des performances des micropuces, leur disponibilité à court ou à moyen terme n'est pas nécessairement acquise.

Les terres rares : un enjeu commercial et politique

Les terres rares sont un ensemble de 17 éléments présents dans certains minerais et essentiels à de nombreux produits : électronique, turbines, lentilles de caméra, aimants... Ils ne sont pas particulièrement rares, mais leur concentration au sein des minerais correspondant est faible, rendant leur extraction plus difficile que des métaux plus conventionnels. En effet, les minerais ne sont pas homogènes mais composés de plusieurs types de terres rares, en sus de matières radioactives telles que le thorium et l'uranium. L'extraction des terres rares nécessite notamment l'usage de matières toxiques (sulphates, ammoniaque, acide hydrochlorique, etc.), ayant un impact environnemental important, raison pour laquelle les États-Unis ont historiquement cessé toute extraction au bénéfice d'importations.

La Chine a longtemps profité de l'absence de contrôles environnementaux pour extraire et commercialiser ces minerais à bas prix, la propulsant en tête des producteurs mondiaux. Le pays a commencé les extractions à grande échelle dans les années 1980 et représente aujourd'hui 60% de la production dans le monde. Ce chiffre s'inscrit néanmoins dans une tendance à la baisse puisqu'il se portait à plus de 97% en 2010. En effet, outre une prise de conscience de l'environnement par les autorités chinoises, avec notamment la création d'une taxe à l'exportation, la suspension de leurs exportations vers le Japon, pour cause de différends territoriaux, a alerté la communauté internationale sur le risque de domination d'un seul pays sur la chaîne de production mondiale.

Aujourd'hui, les États-Unis cherchent à renverser la tendance et à sortir de leur situation de dépendance. Ils financent ainsi plusieurs projets d'usines de raffinement de minerais de terres rares sur leur propre sol. Leur part dans la production est de 15%, devant la Birmanie (12%) et l'Australie (7%), mais loin derrière la Chine.

Les semi-conducteurs : un marché de plus en plus tendu

De nombreux secteurs industriels font aujourd'hui face à une pénurie de composants. Une grande partie des chaînes de production de produits intégrant l'outil informatique se trouve ainsi régulièrement à l'arrêt, faute d'approvisionnement en micropuces. Cette situation reflète une dépendance systémique grandissante à l'outil numérique : on ne produit plus l'objet si l'on ne peut pas lui accoler son composant numérique.

Cette pénurie est notamment la conséquence d'une tendance de fond marquée par l'augmentation de la demande de composants numériques, à laquelle est venue s'ajouter du fait de la crise sanitaire une forte fluctuation de la demande (plus précisément, une baisse drastique suivie d'une forte augmentation) qui a perturbé la chaîne de production. De façon plus générale, la chaîne d'approvisionnement en semi-conducteurs a été fragilisée par la mondialisation de l'industrie qui a provoqué une concentration des acteurs, avec une nette domination de Taïwan. Du fait de la haute technicité des chaînes de production de semi-conducteurs,

les constructeurs estiment actuellement que le précédent équilibre entre l'offre et la demande ne sera pas retrouvé avant 2023. Cette situation fait aujourd'hui réagir d'autres régions développées du monde, qui développent des stratégies pour héberger sur leur sol des capacités de production, principalement étrangères.

La question de la consommation énergétique

Le numérique est un grand consommateur d'électricité. De ce fait, sa croissance exponentielle n'est soutenable ni dans un monde aux ressources finies, ni au vu de l'état actuel des technologies. On peut d'ailleurs noter que le numérique entre en concurrence avec les technologies de production d'électricité renouvelable sur la question de l'approvisionnement en terres rares.

Cette situation appelle au développement d'alternatives technologiques offrant la meilleure efficience énergétique possible. Dans ce cadre, l'émergence de l'informatique photonique, qui substitue le faisceau lumineux au courant électrique, est un candidat idéal. La disparition de l'effet Joule diminue en effet les pertes électriques tout en réduisant le besoin de refroidissement, lui-même consommateur en énergie. Il n'existe cependant pas encore de modèle viable de transistor optique offrant une meilleure performance énergétique que ceux à base de semi-conducteurs.

Les goulots d'étranglement du numérique, bien réels, ne semblent donc insurmontables qu'au regard du niveau technologique actuel. Les solutions, en partie identifiées, restent à développer, alors que paradoxalement leur développement est tributaire des capacités numériques à disposition. Dans ce cadre, il n'a jamais été aussi important pour les États d'assurer la stabilité de la chaîne d'approvisionnement.

FOCUS INNOVATION

Bodyguard : l'analyse contextuelle au service de la lutte contre le cyber harcèlement

Entretien avec Matthieu Boutard, Directeur général de Bodyguard

Présentation

Bodyguard est une startup française créée en 2018 par Charles Cohen, ingénieur autodidacte, qui s'est saisi de la problématique du cyber harcèlement pour proposer une solution capable de détecter en temps réel les contenus haineux sur Internet.

Elle repose sur le constat que les solutions existantes de modération des contenus ne sont pas en mesure de répondre aux défis actuels du cyber harcèlement, qu'ils soient conjoncturels (actualités marquées par des sujets sociétaux controversés sur fond de racisme ou d'homophobie, croissance exponentielle du harcèlement

en ligne) ou structurels (utilisation grandissante d'un nouveau langage dit « simplifié[1] » sur les réseaux sociaux). Dans ce contexte, les individus sont concernés à double titre : en tant qu'auteurs de contenus d'une part, avec le développement d'un phénomène d'autocensure de journalistes et de jeunes utilisateurs qui n'osent plus exprimer leur opinion sur Internet, et en tant que destinataires et potentielles victimes de cyber harcèlement d'autre part, puisqu'on constate que de plus en plus de contenus haineux s'adressent directement à une personne et non à un collectif.

Bodyguard lance en 2018 une application mobile gratuite à destination des individus et des familles. En 2019, une levée de fonds de 2M€ en amorçage permet à la startup d'envisager un nouveau *business model,* avec la commercialisation en 2020 d'une solution destinée aux entreprises.

La société compte aujourd'hui 20 salariés, 55 000 utilisateurs de son application mobile en France et 5 000 à l'étranger, ainsi qu'une dizaine d'entreprises clientes dans les secteurs des réseaux sociaux et des médias, de l'industrie du jeu-vidéo et du sport. Elle est capable de traiter toute forme de discours de haine y compris la misogynie ou le sexisme, et est accessible dans différentes langues (français, anglais, italien, espagnol et portugais).

Solution

La technologie

Alors que les principaux outils de contrôle des contenus reposent sur le *machine learning* pour détecter et calculer mathématiquement le taux de contenu haineux dans un discours, Bodyguard propose une technologie également basée sur l'intelligence artificielle (IA) mais capable de remettre chaque contenu dans son contexte, de distinguer les mots tendancieux utilisés à contresens dans des situations positives, ou encore d'identifier la cible du message haineux, qu'il s'agisse d'un individu ou de son entourage, d'un groupe ou d'une communauté, pour justifier ses décisions de suppression ou non des contenus[2].

Ce processus de détection des contenus haineux se décompose en quatre étapes :

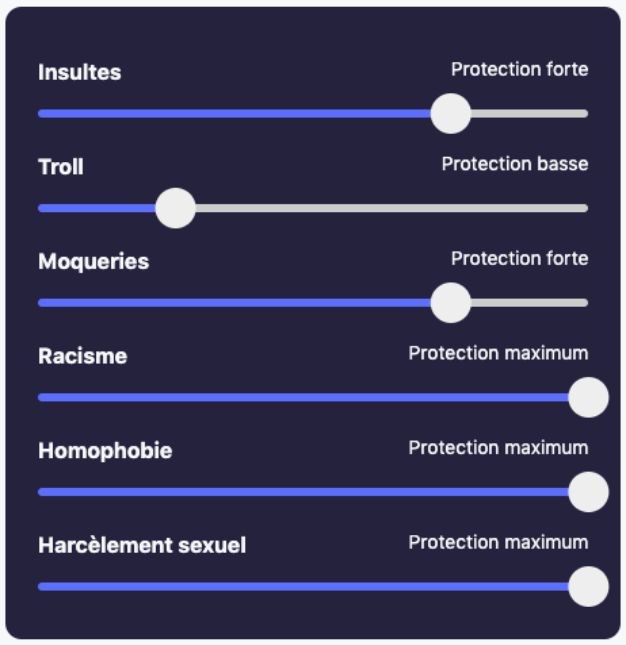
1. Nettoyage des termes du contenu analysé (emoji et fautes supprimés) pour simplifier le travail de recherche ;
2. Recherche des termes, groupes ou associations de mots haineux ;
3. Analyse contextuelle de ces mêmes mots haineux ;
4. Application des règles de modération selon les critères de sévérité adaptés à chaque utilisateur, de l'étudiant à l'homme politique, en passant par l'entreprise ou le groupe religieux.

Deux contenus similaires peuvent ainsi donner lieu à des analyses différentes selon le contexte dans lequel ils sont écrits et publiés, mais aussi selon la sensibilité de chaque utilisateur, qu'il renseigne via un système de curseurs sur son tableau de bord (voir image ci-dessous).

Bodyguard analyse sur cette base la répétition des termes tendancieux, et veille l'actualité afin de détecter si une situation particulière nécessite une augmentation des curseurs de modération de sa part.

[1] Le langage simplifié utilisé sur les réseaux sociaux, composé d'acronymes et d'argot, vient s'opposer au langage parfait qui traduit purement et simplement la langue française classique

[2] Bodyguard assure +90% des contenus de haine et 2% de faux positifs



Curseurs Bodyguard

La solution est aussi considérée comme évolutive dans le sens où elle s'alimente en permanence des nouveaux mots détectés sur les réseaux sociaux pour les intégrer dans son processus de modération en temps réel[3].

Les utilisateurs

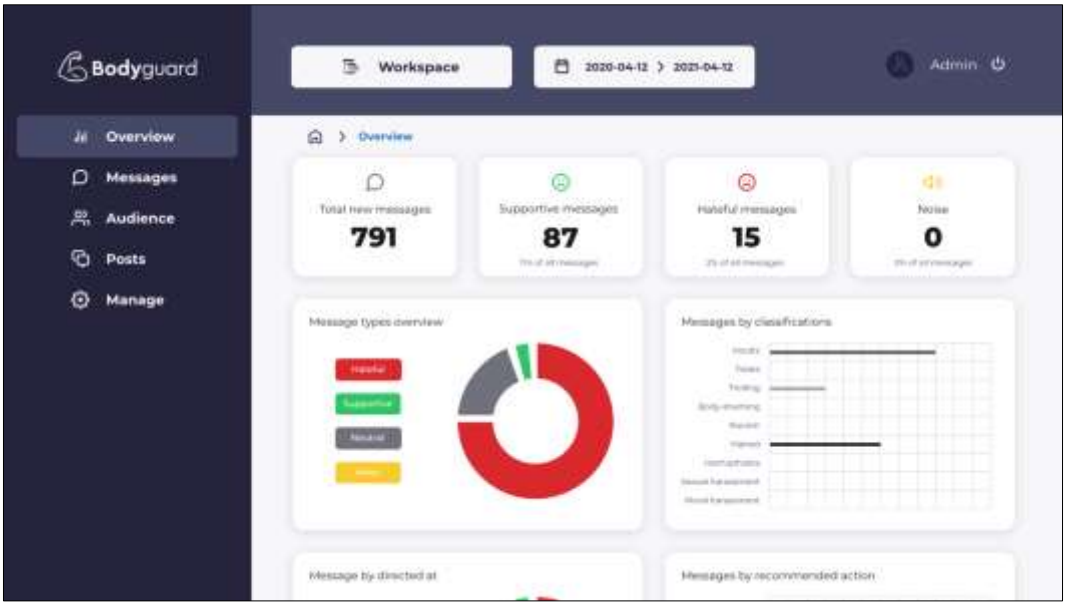
Cette solution est destinée à trois publics : les individus, les familles et les entreprises.

- Pour les individus, Bodyguard s'attache à garantir une application mobile gratuite et adaptée aux besoins de chacun. Tout utilisateur est libre de paramétrer ses propres curseurs afin de les adapter à son environnement ou à ses préoccupations. L'objectif est d'éviter toute forme d'autocensure.
- Pour les familles, la startup se place dans une logique d'éducation en proposant un système d'alerte aux parents dès qu'un de leur enfant est victime ou auteur de cyber harcèlement (sans pour autant dévoiler le contenu des messages afin de respecter la vie privée de ce dernier s'il a plus de 15 ans). Seules les associations de protection de l'enfance avec lesquelles Bodyguard travaille ont accès à ces données dans le cadre d'un accompagnement qui peut être mis en place à la demande des parents. Par ailleurs, la startup est en train de développer un système de gaming pour encourager les jeunes à un usage plus responsable des réseaux sociaux[4].
- Pour les entreprises, Bodyguard analyse les réseaux sociaux à tous les niveaux de l'organisation (dirigeants, employés, réseaux de l'entreprise) ou en s'intégrant directement dans la plateforme de ses utilisateurs sous la forme d'une API classique. La startup soumet aussi des recommandations à l'attention des entreprises n'ayant pas de dispositif dédié en matière de lutte contre le harcèlement, et propose le

[3] Bodyguard a récemment détecté que des groupuscules malveillants avaient transformé le mot « arabe » par « arbre » et avaient créé un champ lexical pour converser autour de la religion

[4] L'idée est d'encourager les jeunes à être bienveillants en ligne, via un système de coins virtuels pour tout comportement positif, toute aide envers des personnes harcelées. Ces coins virtuels sont ensuite transformables en cadeaux offerts par des personnalités connues sur les réseaux sociaux par exemple

Dashboard le plus adapté possible à leurs objectifs (voir image ci-dessous). L'entreprise choisit enfin les niveaux d'accès de ses collaborateurs à ce dernier (pas de limite en termes d'accès, seule la volumétrie du nombre de messages analysé est quantifiée).



Dashboard Bodyguard

Perspectives

Si Bodyguard se concentre aujourd'hui sur l'analyse du texte, elle compte s'étendre aux contenus vocaux/vidéos, et à d'autres langues.

Pour cela, une nouvelle levée de fonds en Série A est envisagée en 2021 et permettra, outre le développement de nouvelles technologies, de s'attaquer à d'autres marchés étrangers ; les États-Unis en priorité, l'Asie ensuite.

Enfin, les élections présidentielles américaines de 2021 ont rappelé les dangers liés à l'influence grandissante des réseaux sociaux et les risques d'ingérence étrangère sur les processus électoraux. La guerre contre la désinformation et les attaques à l'encontre des candidats sont devenus des enjeux majeurs de toute campagne politique. Aussi, dans la perspective de l'élection présidentielle en France, Bodyguard souhaite proposer ses services aux parties prenantes, cabinets de campagne notamment.

ACTUALITÉ

PFUE : Quel rôle pour la cyberdéfense militaire en Europe ?

Compte-rendu du petit-déjeuner du 21 avril 2021

Le cyberespace est le théâtre d'une conflictualité débridée et assumée où s'affrontent des acteurs privés comme publics. L'Union européenne (UE), forte de plusieurs avancées récentes en matière de cybersécurité (directive NIS, boîte à outils cyber-diplomatiques, réseaux de coopération entre États membres…) ambitionne également de s'imposer en acteur incontournable dans ce domaine. Les enjeux sont nombreux : il s'agit à la fois d'assurer sa propre défense et sécurité, contribuant à la résilience de l'Union et celle des États membres ainsi qu'au développement d'une souveraineté numérique. Alors que la France s'apprête à prendre la présidence du Conseil de l'Union européenne en janvier 2022, quel rôle peut-elle jouer pour accélérer la montée en puissance de la cyberdéfense en Europe, et notamment dans sa dimension militaire, moins connue mais non moins stratégique ? Comment peut-elle contribuer à l'affirmation d'une Europe souveraine et indépendante en matière de cyberdéfense et plus largement de numérique ?

Pourquoi parler de cyberdéfense militaire européenne ?

Le manque de visibilité dont souffre l'UE en matière de défense, et à plus forte raison en matière de cyberdéfense n'est pas synonyme d'inaction : elle met en place depuis plusieurs années des mécanismes politiques, opérationnels et capacitaires qui, sans doublonner ceux de l'OTAN, les complètent pour contribuer à affirmer sa place, y compris dans le cyberespace.

Loin d'être concurrentes, les deux organisations sont complémentaires, et affichent même une réelle volonté de coopérer. On ne doit donc pas parler de la cyberdéfense de l'Union européenne, mais bien d'une cyberdéfense européenne, une cyberdéfense des États membres, articulée autour de standards, d'objectifs, de capacités et bientôt d'une analyse des menaces partagée (cf. Boussole stratégique).

Il faut distinguer, mais pas dissocier, cyberdéfense civile et cyberdéfense militaire. Il s'agit plutôt d'un continuum civilo-militaire, dans lequel s'inscrivent non seulement les opérations et les missions, mais aussi les systèmes qui sont défendus dans ce cadre. L'UE est à ce titre la structure au sein de laquelle cette dualité civilo-militaire s'exprime le plus facilement.

Comment se traduit l'ambition européenne en matière de cyberdéfense militaire ?

L'ambition européenne en matière de cyberdéfense comprend un volet conceptuel/doctrinal et un volet capacitaire.

L'état-major de l'UE (EMUE) a initié depuis 2016 une mise à jour des concepts et doctrines de l'UE en matière de cyberdéfense et, depuis 2019, l'élaboration d'une Vision et d'une Stratégie pour l'opérationnalisation du cyberespace : la *EU Military Vision and Strategy on Cyberspace as a Domain of Operations,* par laquelle l'UE se dote des moyens d'affirmer ses ambitions dans le cyberespace. Celle-ci reflète l'aspiration de l'Union à plus d'autonomie, et traduit ses velléités de coopération avec ses partenaires, à commencer par l'OTAN, de développement capacitaire, ainsi que sa volonté de décourager les actes malveillants dans le cyberespace et de développer un continuum civilo-militaire cohérent avec sa doctrine de gestion de crise.

Le volet capacitaire est piloté par l'Agence européenne de défense (AED). Elle a notamment mis en place un processus de développement visant à établir un bilan capacitaire au sein des États membres afin d'identifier

et de combler les lacunes, ainsi qu'un mécanisme de soutien à la R&T. L'AED mène aussi des études et projets destinées à anticiper les futures capacités dont devrait se doter l'UE, y compris en termes de formation et d'entraînement.

Certaines limites internes à l'UE freinent cependant ces ambitions :

- l'éclatement des responsabilités entre les acteurs de sa cyberdéfense ;
- le manque de personnel dédié ;
- le foisonnement d'initiatives difficiles à coordonner.

Quel rôle pour la France, notamment via le COMCYBER, dans le cadre de la PFUE, pour répondre à ces enjeux et développer la dimension militaire dans le domaine cyber ?

L'enjeu principal pour la France sera d'apporter cohérence et coordination aux très nombreux projets et initiatives en cours.

- Définir concrètement le besoin de l'UE en la matière, notamment grâce aux travaux doctrinaires en cours qui permettront de traduire concrètement les ambitions de l'UE en matière de cyberdéfense militaire ;
- Développer ses outils, tant organisationnels que capacitaires, comme le Cyber and Information Domain (CID) Coordination Center CIDCC ;
- Entraîner ces mêmes outils pour œuvrer à la résilience de l'UE en la rendant performante et efficace en situation de crise. Le MIC, exercice annuel des CERT militaires de l'UE, avec sa dimension capacitaire, organisationnelle et stratégique, en constitue la pierre angulaire.

La PFUE sera aussi l'occasion pour la France d'initier un rendez-vous annuel de niveau stratégique et militaire, rassemblant les Cyber Commandeurs européens et permettant de lancer une réflexion stratégique, tant sur les travaux menés que sur les défis futurs à relever.

Ce souci de cohérence souligne aussi la nécessité d'établir une gouvernance unique des SIC et du numérique, indispensable pour palier la dispersion des responsabilités en la matière. La PFUE sera l'occasion de mettre en place une structure dédiée chargée d'initier une véritable réflexion sur le sujet entre les États membres, dans l'objectif d'élaborer ensemble un modèle durable.

La PFUE constitue donc une réelle opportunité pour la France de participer à la structuration de nombreuses initiatives, ainsi que des projets en cours, et contribuer à la mise en cohérence et à l'organisation du dynamisme européen. Mais au-delà des développements capacitaires doctrinaires, il s'agit aussi pour la France de mettre son expérience, notamment celle du COMCYBER, au service de la réalisation d'objectifs opérationnels au niveau européen, pour faire de l'Europe un acteur incontournable de la cyberdéfense militaire.

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