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

Table des matières

ANALYSES (1/2)

COVID-19 OU LE BIG BANG DE LA TRANSFORMATION NUMERIQUE

La crise Covid-19 s'est traduite par une accélération de la numérisation. Même si tous les usages qui ont émergé ou explosé ces derniers mois ne survivront pas à la fin de la crise, le digital sera demain encore plus présent dans nos usages privés et professionnels, et encore plus imbriqué au monde physique. À terme, processus numériques et physiques ne feront plus qu'un. Le digital sera aussi naturel que l'oxygène que l'on respire.

La crise Covid-19 ne fait finalement que préfigurer et accélérer la venue de cet âge de maturité numérique, qualifiée par certains de « post-digitale ». Plus qu'une simple évolution, il s'agit d'un changement de paradigme : l'Humain ne cherche plus à ajouter une surcouche numérique à la vie réelle. Il influe directement sur l'environnement physique en créant des processus hybrides, par exemple en embarquant de façon native du numérique dans des équipements industriels pour mieux les opérer ou les maintenir. Quels sont les premiers enseignements de la crise sanitaire au plan numérique ? Quelles sont les caractéristiques de la nouvelle ère qu'elle préfigure ? Quelles sont les technologies qui soutiennent cette hybridation croissante du cyberespace, de l'environnement physique et du monde du vivant ? Quelles en sont également les limites ? Quelles conséquences sur l'environnement numérique dans lequel opèrent les armées ?

Cet article est une synthèse du 1er webinaire intitulé « Covid-19, big bang de la transformation numérique » du séminaire Cyberdéfense et stratégie. Ce webinaire est accessible en replay *ici*.

1. Une accélération sans précédent des usages numériques

« *Nous venons d'assister à deux ans de transformation numérique en deux mois* » – Satya Nadella (Microsoft)

La crise Covid-19 et le confinement de 3 milliards d'individus ont entrainé une accélération sans précédent des usages numériques. Ces nouvelles formes de travail, de médecine, de sociabilité, de loisir etc. ont même été la clé de voute de la continuité d'activité et de la résilience sociétale.

Trois exemples d'usages : le télétravail, dont en parle depuis longtemps mais qui était resté embryonnaire, a été multiplié par 7 pour atteindre 20 millions de télétravailleurs en France pendant le confinement ; les téléconsultations, qui peinaient à s'imposer avant la crise, sont passées de 20 000 par mois à 1 million en

France au mois d'avril ; certaines installations industrielles ont été télé-opérées à distance avec succès, évitant aux opérateurs une présence permanente sur place.

H4D, expert en télémédecine

Fondée par le docteur Franck Baudino, H4D est spécialisée dans la mise au point et le déploiement de cabines de téléconsultation. Objectif : faciliter l'accès de malades n'ayant pas accès aux professionnels à des consultations à distance, tant pour des soins de médecine générale ou que spécialités, grâce à des cabines installées par exemple dans des mairies, des centres de santé ou des résidences pour personnes âgées. Le service proposé fonctionne sur 3 piliers : l'instrumentation, avec une cabine équipée d'une vingtaine de capteurs permettant au médecin d'effectuer des examens cliniques, la formation, grâce à la mise au point de protocoles médicaux guidant les médecins dans l'utilisation de ces technologies, la construction d'un véritable projet médical autour des cabines, l'objectif étant d'intégrer ces cabines dans un écosystème médical existant, hospitalier ou libéral.

Retrouvez l'article dédié à H4D ici et l'intervention du Dr Baudino ci-dessous :

2. Des infrastructures et des services qui ont encaissé le choc

Cette accélération des usages numériques n'aurait pas été possible sans les infrastructures de communication et des services, qui se sont révélées particulièrement résilientes pendant la crise. Non seulement le réseau Internet, dont certains prédisaient l'effondrement, a tenu, mais les services ont eux aussi, à quelques exceptions près, résisté à une brutale augmentation de la demande.

Pour Stéphane Bortzmeyer, ingénieur à l'AFNIC, l'architecture Internet a ainsi démontré sa résilience. Son maillage dense et étendu permet de faire face à des situations inédites, qu'il s'agisse d'augmentation des usages, de pannes matérielles, d'attaques en déni de service, voire de catastrophes naturelles.

Retrouvez l'intervention de Stéphane Bortzmeyer en cliquant ci-dessous :

Au niveau des entreprises, ce sont là-aussi les architectures Internet et le recours massif au cloud public et à des applications SaaS qui ont permis d'effectuer la bascule très rapide vers le télétravail. « *Du jour au lendemain, le siège s'est vidé. En France, ce sont 20 000 personne qui ont dû travailler chez elle. On était prêt au plan technologique. Depuis 2012, nous avions fait le choix de solutions SaaS sur du Cloud public* », explique Didier Bove, DSI du groupe Veolia.

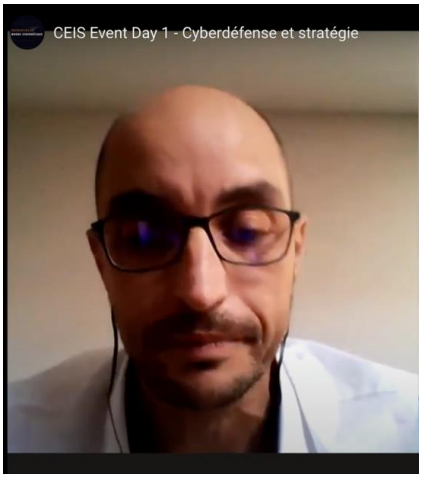
Retrouvez l'intervention de Didier Bove en cliquant ci-dessous :

Un point confirmé par Jean-Christophe Laissy, Directeur et *partner* au sein du Boston Consulting Group (BCG) : *« certaines entreprises étaient prêtes car elles avaient anticipé beaucoup de choses. Beaucoup, en revanche, ont éprouvé des difficultés à augmenter les flux utilisateurs et étoffer leurs VPN. Le VPN n'est pas la technologie la plus moderne qui survivra à la crise. C'est un peu la technique du pont-levis face à la surveillance permanente que permettent aujourd'hui les approches zero trust* ». Objectif : identifier, authentifier et surveiller l'utilisateur en continu, pas simplement à l'entrée de l'entreprise, pour rendre la sécurité plus efficiente mais aussi plus transparente pour l'utilisateur.

3. Le défi de la cybersécurité

Certaines organisations qui n'étaient pas préparées ont ainsi dû faire un arbitrage entre continuité d'activité et cybersécurité, en général au détriment de la seconde. « *Le télétravail a un impact important en termes de sécurité car on se confronte à l'environnement personnel des utilisateurs* », souligne ainsi Benjamin Delubac, RSI et RSSI au Centre Hospitalier Alpes-Isères.

Retrouvez l'intervention de Benjamin Delubac en cliquant ci-dessous :



« *Le principe, c'est l'analyse de risque en continu et la supervision en temps réel de la sécurité. Nous avons déployé des VPN et des outils de virtualisation applicative. Nous avons isolé les flux réseau, déployé des clients sur les postes de travail pour vérifier leur intégrité. Certains ordinateurs personnels équipés de XP, au mieux de Windows 7 ont été écartés* », poursuit-il. Le *Bring Your Own Device* (BYOD) a ainsi montré ses limites pendant le confinement. « *Pour fonctionner de façon fluide, la priorité reste de basculer vers des architectures web et de faire le choix d'une architecture « zero trust », avec un découplage du hardware et du software pour travailler depuis n'importe quel objet de connexion. Le BYOD n'est qu'une conséquence, en aucun cas un projet d'entreprise* », poursuit Jean-Christophe Laissy.

Retrouvez l'intervention de Jean-Christophe Laissy en cliquant ci-dessous :

Cloud public ne rime pas non plus forcément avec sécurité. Si les grandes plateformes offrent globalement un bon niveau de sécurité en matière d'accès, il faut encore que les entreprises utilisatrices disposent des compétences nécessaires en interne pour maitriser les technologies assurant la sécurité à l'intérieur du cloud. Il faut ainsi distinguer la sécurité « du » cloud, maitrisée par les offreurs de service cloud, et la sécurité « dans » le cloud, qui repose en large partie sur les clients, avec des écarts importants selon les entreprises.

4. La crise Covid-19, révélateur de nos dépendances numériques

Au-delà des impératifs de cybersécurité opérationnelle, se pose aussi la question de la dépendance aux grandes plateformes de cloud public, principalement américaines, et donc de notre souveraineté numérique. Certes, cette dépendance n'est pas nouvelle : les acteurs américains dominent les technologies de l'information mondiale depuis les années 70. Certes, qu'il s'agisse d'opérateurs cloud ou de grands éditeurs, les DSI sont habitués à gérer des dépendances fortes : « *on fait des choix qui durent 10 ans. On est de fait dépendant d'un éditeur, d'un opérateur* », explique Jean-Christophe Laissy, du BCG. Mais la crise Covid 19 a servi de révélateur : cette dépendance ne concerne plus uniquement des processus et fonctions support, mais aussi certaines fonctions essentielles d'une organisation. Le numérique a en effet progressivement étendu son périmètre et touche maintenant les « opérations » elles-mêmes. D'où l'importance de sensibiliser les COMEX à ces enjeux de transformation numérique. En matière de choix de fournisseurs ou d'opérateurs, notamment cloud, les décisions ne sauraient relever des simples opérationnels : s'ils sont fonctionnels, technologiques et financier, ces choix sont avant tout stratégiques car c'est la survie de l'entreprise qui est en jeu.

Il ne faut pas non plus se bercer d'illusion, car les options sont de fait limitées: en matière de cloud public, les grands groupes internationaux n'ont souvent d'autre choix que de recourir à des solutions ayant une couverture mondiale, ce qui exclut bien souvent les opérateurs européens. La solution est donc souvent dans une approche « multicloud », consistant à choisir différentes solutions en fonction de types de données concernées et des risques associés. D'abord relativement théorique, cette approche apparait de plus en plus mature. « *Le multicloud va devenir une réalité intangible assez rapidement grâce aux fournisseurs qui sont beaucoup moins dans une logique de silotage que les acteurs « legacy » historiques* », souligne Jean-Christophe Laissy. Les grands acteurs proposent ainsi de plus en plus des offres SaaS tournant sur les infrastructures d'autres opérateurs, et réciproquement. « *Il est donc possible aujourd'hui de mettre en place des stratégies multicloud voulues, et non subies* », poursuit-il.

5. Et après la crise ?

Si tous les usages qui ont émergé ou ont explosé pendant la crise ne lui survivront pas tous, l'accélération de la transformation numérique pendant le confinement aura des conséquences durables. La crise a en outre eu le mérite de mettre en lumière certaines des limites de la transformation numérique.

Au plan sociologique, la généralisation du télétravail conduira sans doute à la définition d'un nouveau cadre juridique, déjà amorcé par les « Ordonnances Macron » de 2017 qui avaient déjà donné à un coup de pouce à cette pratique pour permettre aux employeurs de faire face aux grèves et pics de pollution. *« La période va sans doute induire une obligation sur l'équipement du télétravailleur à domicile »,* explique Camille Rabineau, consultante LMGB Worklabs. La définition du télétravail, simplement aujourd'hui conçu comme le déplacement sur son domicile des mêmes méthodes et du même fonctionnement que le travail « sur site », devrait aussi être revue. L'objectif étant que le télétravail, qui a été plus subi que choisi pendant la crise, soit mis en place sur la base d'un double volontariat : celui de l'entreprise et du salarié.

Retrouvez l'intervention de Camille Rabineau en cliquant ci-dessous :

Il s'agit aussi de maitriser les effets néfastes du télétravail, largement observés pendant le confinement. Comme le note Didier Bove: dans les premiers jours, on travaille à la maison comme au bureau ; au bout de quelques jours, on commence de plus en plus tôt et on finit de plus en plus tard, au point que l'on perd parfois pied par rapport à son environnement. « *Nous avons donc dû mettre en place des règles, comme par exemple le fait que les sessions de visio-conférence ne devaient pas excéder 55 minutes ou que la pause déjeuner était obligatoire* ». Dans un 3ème temps, enfin, il devient essentiel de rééquilibrer la balance entre l'accès aux outils numériques et le besoin de lien social pour « refaire société ». Le bilan du télétravail est donc contrasté avec d'un côté des effets positifs et de l'autre des conséquences néfastes (isolement, douleurs

lombaires, baisse de la communication, confusion des sphères professionnelles et personnelles…). Selon un sondage Opinion Way sorti en mai, 39% des travailleurs se sont ainsi sentis isolés. 53% étaient en attente de davantage d'encadrement. Pour que le télétravail soit positif pour les deux parties, il faut donc adapter les modes d'organisation et de management pour donner plus d'autonomie aux salariés, tout en veillant à maintenir entre eux les liens sociaux et à faciliter l'identification à leur organisation.

Au plan technologique et industriel, la prise de conscience de notre forte dépendance aux grands acteurs américains va également nous conduire à « opérationnaliser » le débat souvent très théorique sur la souveraineté numérique européenne. Parce qu'il nous est impossible de rivaliser avec les budgets de R&D colossaux des grandes plateformes, l'objectif sera surtout de concevoir et mettre en place un « cloud de confiance » pour héberger certains types de données sensibles, tout en mettant l'accent sur les « couches hautes », c'est-à-dire sur le développement logiciel et les applications SaaS, afin de conserver la maitrise de nos données. *« L'intelligence de la donnée est dans l'application, pas dans les couches de l'infrastructures »,* note Jean-Christophe Laissy.

ANALYSES (2/2)

AFFRONTEMENTS INFORMATIONNELS : UNE NOUVELLE DONNE GEOPOLITIQUE ?

La guerre de l'information est une combinaison d'actions humaines ou technologiques destinées à l'appropriation, la destruction ou la modification de l'information selon trois logiques : manipulation de la connaissance, maîtrise des canaux de diffusion et interdiction d'émission[1].

L'attaque informationnelle[2] est un outil de la guerre de l'information. Elle désigne « une action délibérée et limitée dans le temps visant à utiliser la connaissance contre un adversaire choisi. […] phénomène rumoral visant à nuire intentionnellement à une entité identifiable, ou à ses intérêts ». Elle permet de poursuivre simultanément des objectifs de plusieurs natures : économiques, technologiques, militaires, réputationnels, etc. Selon Daniel Ventre il s'agit de « toute activité destinée à acquérir données et connaissances (et à en priver l'adversaire) dans une finalité stratégique, soit par des systèmes (vecteurs et moyens de traitement de l'information), soit par le contenu, en assurant une domination informationnelle[3] ».

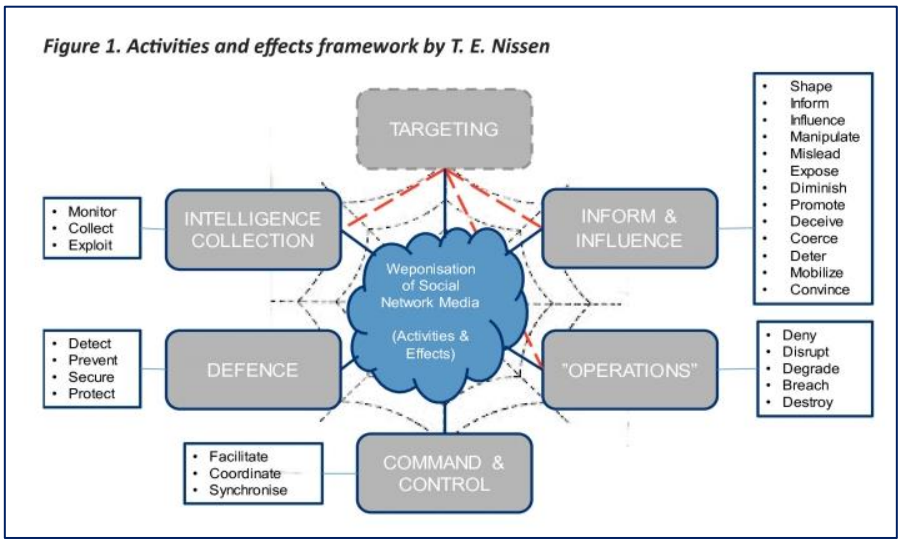
L'attaque informationnelle peut prendre différentes formes, que ce soit une action de propagande (si elle est dirigée vers ses propres partisans), d'intoxication, de leurre, de calomnie ou de désinformation. Elle s'appuie sur divers outils tels que les cyberattaques, les vols de données, la propagande, ou la manipulation de l'information, entre autres.

Dans ce contexte où l'environnement informationnel et en son sein le cyberespace deviennent des terrains d'affrontement pour les États comme pour les acteurs non étatiques, les attaques informationnelles constituent autant d'outils au service d'acteurs en recherche d'influence culturelle, civilisationnelle, ou commerciale.

[1] https://portail-ie.fr/resource/glossary/97/guerre-de-linformation
[2] https://portail-ie.fr/resource/glossary/86/attaque-informationnelle
[3] https://www.iris-france.org/note-de-lecture/cyberguerre-et-guerre-de-linformation-strategies-regles-enjeux/

Les réseaux sociaux, nouveau théâtre des affrontements informationnels

Les réseaux sociaux sont aujourd'hui à la fois les principaux vecteurs et outils de la guerre de l'information que mènent les acteurs étatiques et non étatiques dans le cyberespace[4].



Le visuel ci-dessous, proposé dans le rapport de l'OTAN de 2016 « Social media as a tool of hybrid warfare » présente les différents modèles et l'ADN d'une attaque informationnelle[5].

Les différents acteurs y poursuivent des objectifs multiples : discréditer un adversaire, en temps de guerre mais surtout en temps de paix, assoir des intérêts politiques, économiques et diplomatiques, imposer et diffuser un narratif auprès d'une population… Tous ces objectifs répondent *in fine* à un impératif de domination informationnelle qui, dans un contexte militaire, s'impose comme la composante indispensable de la domination opérationnelle lors d'un conflit :

- Qu'il s'agisse d'un conflit armé, comme le cas de l'Ukraine et de la Russie : la guerre de l'information a fait rage sur les réseaux sociaux russophones dans le cadre du conflit en Crimée. Au-delà des réseaux sociaux russes comme VKontakte, les réseaux Twitter et Facebook ont été largement investis par des « trolls » qui ont notamment créé des faux profils et des faux comptes pour amplifier les narratifs russes dans le but de délégitimer les manifestations pro-européennes au profit d'une intervention russe[6] ;

- Qu'il s'agisse d'un conflit politique et territorial non armé, comme c'est le cas à Hong Kong. Une campagne de désinformation contre Hong Kong, orchestrée par le Parti communiste chinois et conduite par des trolls chinois, a par exemple été révélée par Twitter[7]. Elle avait pour objectif de délégitimer le mouvement de manifestation à Hong Kong et promouvoir l'action diplomatique de Pékin.

---

[4] https://www.stratcomcoe.org/social-media-tool-hybrid-warfare rapport de l'OTAN « Social media as tool of hybrid warfare », 2016

[5] https://www.stratcomcoe.org/social-media-tool-hybrid-warfare

[6] https://www.courrierinternational.com/article/russie-une-armee-de-trolls-au-service-de-poutine

[7] https://www.forbes.com/sites/kenrapoza/2020/06/14/twitter-busts-chinas-info-war-campaign-against-hong-kong-pandemic/#17f384559e29

- Qu'il s'agisse enfin d'un conflit commercial dans le cadre d'une compétition globale comme c'est notamment le cas entre la Chine et les États-Unis, qui s'échangent régulièrement des tweets agressifs sur différents fronts (statut des Ouïghours, Coronavirus, Hong Kong, Taïwan…)[8,9]. L'exemple de du conflit commercial autour de Huaweï, accusé d'agir pour le compte de l'Etat chinois, est éloquent[10].

Dans tous ces cas, l'attaque informationnelle doit permettre à la fois de contrer le narratif d'un adversaire et d'imposer le sien auprès de ses alliés comme de ses concurrents.

Les différents acteurs peuvent opérer sur les réseaux sociaux de façon ouverte dite « déclarée » (« overt ») par exemple en communiquant via leurs comptes officiels, ou de façon « déguisée » (covert). Dans cette dernière configuration ils peuvent notamment utiliser de fausses identités et de faux comptes, comme l'a fait l'armée américaine, avec l'aide de l'entreprise Ntrepid, pour diffuser un narratif pro-américain au Moyen-Orient dans le cadre des opérations en Irak et en Afghanistan en 2011[11]. Ils peuvent aussi recourir à des armées de « trolls », parfois sous forme de bots comme décrites notamment par David Patrikarakos dans « War in 140 characters[12] », pour saturer les réseaux adverses de commentaires les discréditant ou de les inonder de leurs propres narratifs (*astroturfing*). C'est par exemple le rôle de la « 50 Cent Army », armée de trolls chinoise, derrière notamment la campagne de calomnie contre Hong Kong[13] (entre 2019 et 2020). Ces mêmes méthodes sont également utilisées dans le cadre d'actions « déclarées », par exemple dans la conception de narratifs pro-Chine dans le cadre du Covid-19 (en avril 2020 notamment). Les messages de ces comptes sont ensuite repris par des médias chinois officiels comme « The Global Times » ou encore par des diplomates comme l'Ambassadeur de Chine à l'ONU à Genève[14]. De même, une armée de trolls liés au régime iranien, a déferlé sur les réseaux sociaux pour s'attaquer aux États-Unis et diffuser une propagande pro-Iran à la suite de la mort du général Soleimani[15]. Plus récemment enfin ce sont les « QAnon », ultra-nationalistes américains, soutenus par des proches du gouvernement, qui inondent actuellement les réseaux sociaux en vue des élections de 2020 pour présenter le narratif pro-Trump tant à l'intérieur des États-Unis qu'auprès d'audience externes.

Certains États exercent même un contrôle direct sur certains réseaux sociaux. C'est par exemple le cas de la Chine sur l'application TikTok, développée par la startup chinoise ByteDance pour le marché international sur la base de sa version originelle chinoise Douyin. Comme toute plateforme chinoise, elle fait l'objet de la censure gouvernementale par le biais de près de 400 « censeurs » chargés de s'assurer de la conformité de ses contenus avec la ligne du Parti communiste chinois. Malgré un modèle présenté comme plus ouvert et permissif, Tiktok n'est pas non plus à l'abri du contrôle de Pékin, accusé d'en avoir fait retirer des contenus

---

[8] https://www.sudouest.fr/2020/03/17/virus-chinois-pekin-indigne-par-le-tweet-de-donald-trump-7336716-4803.php

[9] https://www.franceinter.fr/monde/chine-usa-les-nombreuses-raisons-d-une-guerre-froide

[10] https://www.letemps.ch/opinions/huawei-technologies-coeur-dune-terrible-guerre-froide-numerique

[11] https://www.numerama.com/magazine/18319-l-armee-americaine-veut-manipuler-les-reseaux-sociaux-avec-de-faux-profils.html

[12] http://www.slate.fr/story/158692/gagner-guerre-twitter-facebook-reseaux-sociaux

[13] https://www.forbes.com/sites/kenrapoza/2020/06/14/twitter-busts-chinas-info-war-campaign-against-hong-kong-pandemic/#17f384559e29

[14] https://www.forbes.com/sites/kenrapoza/2020/06/14/twitter-busts-chinas-info-war-campaign-against-hong-kong-pandemic/#17f384559e29

[15] https://www.washingtonpost.com/

allant à l'encontre de ses intérêts[16]. Suite à la promulgation de la récente de la loi « Sécurité nationale[17] » chinoise, dont l'objectif est de lutter contre la subversion, la sécession, le terrorisme et la collusion avec les forces étrangères, la plateforme a tout simplement été suspendue à Hong Kong. Ce nouveau dispositif permet ainsi à la Chine de contrôler l'information et ses narratifs dans une région où la contestation passait avant tout sur les réseaux sociaux.

Les médias traditionnels, et notamment ceux ouvertement et directement liés à certains États, ont également investi les réseaux sociaux. Par exemple, les comptes Twitter de Sputnik, RT ou encore AJ+ sont devenus les principaux relais des événements sociaux liés aux mouvements contre les violences policières en France. Ils accentuent et donnent de l'écho aux critiques, amenuisant la portée du narratif officiel. Ils contribuent directement et amplifient les campagnes de désinformation et de propagande orchestrées par les États.

Les cyberattaques comme vecteurs d'attaques informationnelles

Les cyberattaques, si elles ne sont pas un élément de guerre informationnelle en tant que telles, peuvent dans certains cas être conçues comme des outils au service d'une campagne informationnelle. Elles peuvent dans ce cadre être commanditées directement par des États ou des organisations affiliées, et viser tant des États que des entreprises stratégiques ou des personnalités publiques…

Par exemple, le piratage de plusieurs aéroports vietnamiens[18] dans le cadre du conflit qui oppose le pays à la Chine en Mer de Chine du Sud, imputée à un groupe de pirates commandités par la Chine, a permis de diffuser des messages anti-Vietnam et anti-Philippines sur les écrans et dans les haut-parleurs des principaux aéroports du pays préalablement « défacés ». La cyberattaque a ainsi permis de diffuser un narratif rappelant la souveraineté de Pékin sur la mer de Chine, mais également de décrédibiliser et pointer les failles de sécurité des pays attaqués auprès du public international.

C'est aussi le scénario de l'attaque contre la chaîne TV5 Monde de 2015, qui avait vu les comptes des réseaux sociaux de la chaîne « défacer » le site pour diffuser des messages faisant l'apologie du terrorisme et dénonçant les guerres menées par la France, alors que l'infrastructure de diffusion de la chaîne était hors de service et plus en capacité de diffuser. Le piratage d'une chaîne de télévision peut également se faire de façon plus discrète, via uniquement le site internet de la chaîne. Ainsi une campagne de désinformation anti-OTAN qui reposait sur le piratage de sites de médias officiels (via le Content Management System ou CMS des sites) afin d'y faire publier des faux articles a été découverte en 2020 (sous le nom de « ghostwriter », qui sévirait depuis 2017). Les cyberattaques étaient complémentaires d'autres méthodes : faux mails ressemblant à des mails officiels envoyés, faux journalistes auteurs d'articles ; obligeant des membres de l'OTAN à réagir. Les attaques, méthodes et discours ont poussé certains États à soupçonner une action menée par la Russie, pour discréditer l'OTAN et les États-Unis.

D'autres cyberattaques ont pour objectif le vol de données dans le but de les republier sur les réseaux sociaux. Il est à cet égard important d'évoquer les « Hacking & Leaking Operation[19] » (« HALO »), particulièrement

[16] https://knowledge.wharton.upenn.edu/article/singer-weaponization-social-media/

[17] https://www.lesechos.fr/tech-medias/hightech/le-chinois-tiktok-se-retire-de-hong-kong-les-geants-americains-sur-leurs-gardes-1221844

[18] https://www.bbc.com/news/world-asia-36927674

[19] https://www.lefigaro.fr/vox/politique/la-france-doit-se-proteger-contre-la-desinformation-etrangere-20200604

efficaces en période électorale. On peut citer notamment les fuite d'informations attribuées à la Russie[20] dans le cadre des campagnes des candidat Hillary Clinton et Emmanuel Macron et visant à les discréditer. D'autres « leaks » impliquaient les correspondances mail de l'Internet Research Agency de Saint Petersbourg par le groupe b0ltai.org[21], qui a permis de prouver que l'agence était en fait une fabrique à trolls russes impliqués dans le conflit qui opposait la Russie à l'Ukraine[22].

Exemple d'utilisation étatique de la guerre de l'information : la Chine

La Chine assume pleinement et publiquement sa volonté de maîtriser le cyberespace. Le contrôle de l'information qui y circule est au cœur de sa stratégie comme en témoignent diverses publications de l'administration chinoise du cyberespace[23]. Plus précisément, l'un des objectifs de la Chine consiste à renforcer son contrôle sur Internet au niveau national pour maintenir l'autorité du Parti communiste chinois.

Dans le but d'élargir son contrôle sur l'information et sa propagande au-delà de ses frontières, la Chine se montre extrêmement proactive au sein des différentes organisations internationales pour y imposer ses narratifs[24,25]. Son implication dans le jeu international se traduit d'une part par une stratégie d'entrisme auprès des différentes organisations globales (comme l'OMS), avec la volonté d'accroître son influence auprès de pays considérés comme négligés par les puissances occidentales La Chine mène ainsi une politique agressive sur les questions territoriales combinée à des opérations de séduction. À cet effet, son armée de faux comptes mobilisée sur les réseaux sociaux[26] lui permet aussi bien de diffuser des narratifs de propagande interne ou externe, que de mettre en cause ses adversaires, via notamment les comptes Twitter des médias chinois.

---

[20] https://www.lemonde.fr/international/article/2016/10/17/elections-americaines-que-revelent-les-courriels-d-hillary-clinton-devoiles-par-wikileaks_5015324_3210.html

[21] https://www.stratcomcoe.org/social-media-tool-hybrid-warfare

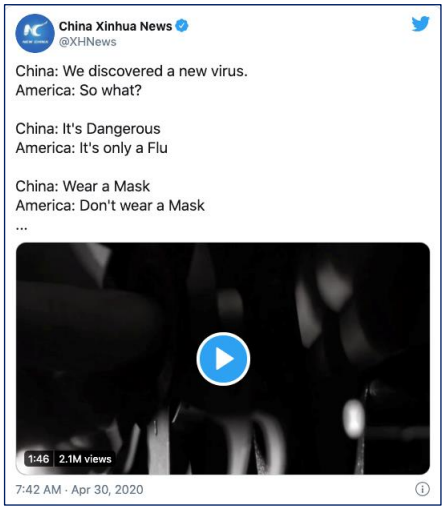
[22] https://www.letemps.ch/monde/diplomatie-fuite

[23] http://www.pircenter.org/media/content/files/9/13512404110.pdf

[24] « Quand Pékin propose une mondialisation alternative », Alice EKMAN, journal Le 1 n°299

[25] Intervention de Nadège Rolland dans l'émission « Affaires étrangères » de Christine Ockrent sur France Culture dédiée à « Chine, Etats-Unis : l'escalade » du 23 mai 2020 avec Alice Ekman, Antoine Bondaz, Benjamin Haddad, Sébastien Jean et Nadège Rolland

[26] https://www.lefigaro.fr/international/cyberattaques-desinformation-surveillance-industrielle-la-grande-offensive-des-espions-chinois-20200717



Le cas de l'Australie est intéressant pour comprendre les méthodes et stratégies chinoises. À la fois un partenaire commercial majeur et cible privilégiée de la Chine[27], elle a subi, après avoir demandé l'ouverture d'une enquête internationale quant aux origines du Covid-19, une série de cyberattaques contre certaines entreprises stratégiques[28], agences gouvernementales, administrations (comme l'Université Nationale d'Australie), partis politiques et le Parlement[29]. L'État australien, sans citer la Chine, a parlé d'attaques menées par un « acteur étatique sophistiqué » et regarde de façon appuyée vers la Chine avec qui les relations se sont dégradées depuis[30]. Les cyberattaques, conçus comme les outils d'un conflit informationnel permettent ici à la Chine d'atteindre plusieurs objectifs simultanément : elles pointent les défaillances de l'Australie, l'obligent à réagir, mais agissent aussi comme une menace et servent de levier de négociation avec le partenaire commercial qu'est la Chine.

Dans le cadre de la crise de Covid-19, le comportement de la Chine dans le domaine informationnel, largement perçu comme agressif par les puissances occidentales, s'inscrit dans un contexte marqué par une recrudescence des attaques à son encontre. Ces attaques, xénophobes et racistes pour certaines, peuvent cacher des activistes proches de certains États, notamment des États-Unis[31], notamment avec de nombreux tweet assimilant Chine et coronavirus imputés à des « bots » de la mouvance QAnon[32]. Dans ce contexte, l'enjeu majeur pour la Chine fût réputationnel, comme le relevaient les sénateurs Olivier Cadic et Rachel Mazuir dans une note de synthèse d'avril 2020[33].

Conclusion

Il faut sans doute s'attendre à une intensification de la guerre de l'information. L'un de ses protagonistes, la Chine, affirme en effet depuis quelques années une volonté d'expansion à la fois politique et commerciale, dont la guerre de l'information est l'un des vecteurs. Dans ce contexte, sa stratégie semble s'articuler autour d'une part d'attaques informationnelles contre ses adversaires et d'autre part de diffusion de narratifs destinés tant à séduire de potentiels partenaires parmi les États dits « développés » en Europe, qu'à promouvoir les bienfaits d'une puissance comme la Chine auprès de pays en développement[34]. C'est le jeu qu'elle a joué en

[27] Rapport conjoint CAPS/IRSEM – « Les manipulations de l'information : Un défi pour nos démocraties », 4 septembre 2018

[28] https://www.lemonde.fr/international/article/2020/07/10/en-depit-des-menaces-de-represailles-l-australie-ne-veut-rien-ceder-a-la-chine-sur-hongkong_6045785_3210.html

[29] https://www.bbc.com/news/world-australia-46096768

[30] https://www.lemonde.fr/international/article/2020/06/19/l-australie-se-dit-victime-d-une-cyberattaque-d-un-acteur-etatique_6043366_3210.html

[31] http://www.opex360.com

[32] https://www.centreforresponsibletechnology.org

[33] https://www.senat.fr/presse/cp20200416b.html

[34] Intervention de Nadège Rolland dans l'émission « Affaires étrangères » de Christine Ockrent sur France Culture dédiée à « Chine, Etats-Unis : l'escalade » du 23 mai 2020.

Europe dans le contexte de la crise Covid-19[35]. La Chine insiste en effet sur sa générosité par la mobilisation de ses capacités industrielles au service des Etats touchés à leur tour par la crise, comme par exemple l'Italie. Et ce à grand renfort de communication sous le terme trouvé à l'époque de « diplomatie du masque[36] ».

La France et l'Europe ont, dans les guerres de l'information, un rôle généralement plus neutre sur les situations, les origines, les raisons et les moyens des attaques informationnelles. La France et l'Europe ont sans doute un rôle régulateur, notamment sur les réseaux sociaux, à jouer dans les affrontements informationnels, encore faut-il qu'elles continuent à l'imposer pour tenir un rôle clé du jeu de l'information[37]. C'est un enjeu pour leur propre souveraineté.

L'un des prochains affrontements susceptibles de justifier une hausse des attaques informationnelles pourrait être la nouvelle course à l'espace. Le développement de narratifs a d'ores et déjà commencé, au vocabulaire guerrier, alors que la Chine tient aujourd'hui le haut du pavé.

FOCUS INNOVATION

H4D : des cabinets médicaux connectés

Présentation

Président et fondateur, le Dr. Franck Baudino a créé la société de télémédecine clinique Health 4 Development (H4D) en 2008. L'entreprise conçoit des cabines connectées qui permettent à un patient de bénéficier d'un examen clinique effectué par un médecin à distance. Destinées à favoriser l'accès aux soins, les cabines H4D sont essentiellement implantées dans les collectivités qui présentent des déserts médicaux (au niveau entre autres des mairies et des résidences pour personnes âgées), mais le sont également de plus en plus au sein d'entreprises (Airbus, Bouygues, Carrefour, Vinci, etc.). Elles permettent aux patients et aux salariés de limiter leurs déplacements pour recevoir des soins.

La solution

Par le biais de ses cabines, H4D livre un service complet qui couvre 99% du périmètre des activités d'un cabinet médical traditionnel. Après avoir pris rendez-vous via une application dédiée ou l'intranet des entreprises équipées, le patient entre dans la cabine et démarre une visio-conférence avec un médecin formé aux procédures d'utilisation du dispositif H4D. Chaque cabine est dotée d'une série d'outils de mesures composée d'une vingtaine de capteurs (prise de tension artérielle, fréquence cardiaque, température, taille, poids, tests visuels et auditifs, etc.). Guidé à distance tout au long de la consultation, le patient participe activement à son examen clinique en effectuant lui-même les mesures nécessaires dont les données sont transmises au médecin. Ce dernier délivre ensuite directement sa prescription qui est imprimée dans la cabine.

---

[35] http://www.opex360.com/2020/05/10 /covid-19-un-rapport-chinois-redoute-une-confrontation-militaire-avec-les-etats-unis/

[36] https://www.lejdd.fr/International/aide-financiere-livraison-de-materiel-pourquoi-la-chine-se-demene-face-a-la-pandemie-de-coronavirus-3958973

[37] https://www.euractiv.fr/section/economie/news/time-to-tell-the-truth-on-chinese-disinformation-jourova-says/

L’innovation

Pour H4D, la technologie ne peut résoudre seule toutes les problématiques de santé. Elle constitue toutefois une brique fondamentale dans l’écosystème médical. Fruit de huit années de recherche et développement (R&D), le dispositif médical de classe 2 développé par H4D, c’est-à-dire de même niveau que ceux des services hospitaliers, s’articule autour d’une cabine (espace de confidentialité) et d’une infrastructure logicielle. Sept années de développement d’un protocole dédié de formation de médecins indépendants (généralistes et spécialistes) viennent le compléter.

Une partie de l’infrastructure logicielle est hébergée dans un *cloud* sécurisé. Outre l’identification du patient et du médecin, le dispositif permet aussi leur mise en relation sécurisée, ainsi que la transmission à sens unique de données de santé cryptées de bout-en-bout. La solution H4D prévoit également une aide au diagnostic basée sur une intelligence artificielle (IA) qui repose sur des données médicales fiables et reproductibles. Ce dispositif permet d’établir des valeurs de prédiction des facteurs d’aggravation et aide ainsi à la prise en charge du patient. Toutes les données de santé stockées le sont chez un hébergeur agréé par le ministère de la Solidarité et des Santés.

Cas d’usage

Dans le cadre de la crise du Covid-19, des algorithmes conçus à partir de plusieurs paramètres (pouls, tensions, températures, poids, taille, âge) ont permis de dégager rapidement des indicateurs fiables de facteurs d’aggravation chez certains patients atteints du virus. Installée par exemple dans le service d’urgence d’un hôpital, la cabine H4D a permis d’optimiser les délais de pris en charge des malades, en distinguant ceux à envoyer directement en salle de réanimation plutôt qu’en salle d’examen.

Ayant vocation à pallier une absence géographique de personnels de santé, plusieurs autres cas d’usage des cabines H4D peuvent être envisagés, parmi lesquels la possibilité d’assurer un suivi médical de troupes à l’étranger, ainsi que de soigner les populations locales sur un théâtre d’opération.

Actualité

H4D s’appuie sur un réseau de plus d’une soixantaine de cabines opérationnelles (France, Europe et Amérique du Nord) et prévoit de dépasser la centaine d’ici quelques mois. Afin de « multiplier ses projets de déploiement et son implantation territoriale », la société a levé en juin 2020 quinze millions d’euros.

Pour plus d’informations, accédez au site officiel de H4D en cliquant ici.

CALENDRIER

Ouverture des candidatures au Grand Défi cyber

L'ouverture des candidatures au Grand Défi cyber pour la première phase des axes verticaux (réseaux, objets connectés et protection des petites structures) est sur le point d'être mise en ligne sur le site de Bpifrance. Le dossier à remplir et davantage de détails y seront disponibles en téléchargement.

Les projets pour ces trois axes seront découpés en deux phases :

- La première, sur le point de démarrer, s'achèvera en janvier 2022. Elle s'étendra ainsi sur 12 à 15 mois de réalisation en fonction de la date de dépôt des candidatures (la sélection se faisant au fil de l'eau) ;
- La seconde correspondra à une « sur-sélection » des dossiers déjà retenus pour la première phase pour n'en retenir que quelques-uns dans une logique d'accélération sur 11 mois (jusqu'à fin 2022).

Le dossier de candidature à fournir est centré sur la première phase et doit mettre en valeur trois aspects :

- Les verrous et les ruptures technologiques ;
- L'ambition de croissance et les projections de commercialisation à court/moyen terme ;
- L'intégration dans l'écosystème (interopérabilités, synergies, etc.).

Vous trouverez plus d'informations, dont la feuille de route du Grand Défi, sur le site officiel en cliquant ici.

Pour toutes questions et informations complémentaires, vous pouvez contacter : gd.cyber@pm.gouv.fr.

ACTUALITÉ

L'Armée de l'Air remporte le premier « Cybercrunch »

Pour la première fois le 9 juillet 2020, l'Armée de l'Air et la Royal Air Force se sont affrontées au cours d'une compétition amicale dans l'espace numérique. Premier exercice de lutte informatique défensive franco-britannique, le « Cybercrunch » a opposé les spécialistes SIC de l'escadron des systèmes d'information opérationnels et de cyberdéfense (ESIOC) 62.430 « Marensin », de la base aérienne 118 de Mont-de-Marsan, et de la *591st Signals Unit* (*591SU*) de la *Royal Air Force.*

Si l'exercice de type « Capture the Flag » a eu lieu dans le cadre du jumelage entre les deux unités et visait à renforcer leurs liens, il s'agissait aussi d'un exercice de lutte informatique défensive destiné à assurer le niveau de préparation opérationnelle. Il nécessitait en effet la mise en œuvre de toute la chaîne des compétences et connaissances sollicitées dans le cadre d'une cyber-opération, de la surveillance à la réponse à incident.

L'ESIOC a remporté la première édition de cette compétition, qui sera reconduite annuellement en sol français ou britannique.

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