Lettre n°67 - Octobre 2017 - disponible sur omc.ceis.eu

TABLE DES MATIERES

NOUVELLES TECHNIQUES DE GEOLOCALISATION ET RISQUES CYBER

La capacité de se localiser dans l'espace est un besoin ressenti depuis des millénaires. Elle a très lentement progressé au cours des siècles avec l'avènement de la boussole, du compas, de la cartographie, de l'astronomie et du chronomètre. Ce n'est qu'au XXème siècle que des progrès considérables ont pu être réalisés. D'abord avec le développement des ondes radioélectriques, qui a permis la radiogoniométrie, avant l'arrivée de grands systèmes terrestres de radionavigation comme le DECCA, le LORAN puis l'Oméga. Puis avec l'utilisation de satellites par le système Transit, dans les années 1960, rapidement suivi par le GPS. Ces systèmes de navigation donnaient à chacun sa position, de plus en plus précisément au fil du temps, mais cette position ne pouvait être connue par d'autres qu'en la leur transmettant, par les coursiers de l'antiquité ou par les messages radioélectriques des temps modernes.

La géolocalisation, c'est-à-dire la capacité à déterminer la position d'un être ou d'un objet, a pu réellement émerger grâce au développement des technologies de l'information et de la communication.

La position est généralement obtenue par une liaison physique, radioélectrique ou sans-fil avec un ou plusieurs points d'accès à un réseau dont on connaît les coordonnés géographiques (adresse IP d'un ordinateur, antennes relais de téléphonie mobile, bornes de communication sans-fil …), et qui sert également à la transmission de cette position vers ceux qui en ont besoin. La précision de ces techniques varie avec la portée de la liaison entre l'objet connecté et le point d'accès au réseau ou la balise. Elle peut être améliorée par triangulation lorsque l'objet peut être relié à plusieurs points, et par la combinaison de plusieurs techniques.

L'avènement des réseaux de téléphonie mobile, dans les années 90, a permis les premières géolocalisations, avec une précision qui n'a cessé ensuite d'augmenter avec la densification des relais de téléphonie et avec la combinaison de la position "GSM" avec celle des bornes Wifi proches. A la même époque, la technologie RFID (radio-frequency Identification) a rendu possible le suivi géographique des objets ou des êtres vivants équipés d'une étiquette RFID lors de leur passage à proximité de portiques dédiés. Le développement de l'Internet, dans les années 2000, a vu également la possibilité de géolocaliser un internaute ou un objet connecté avec son adresse IP.

D'autres techniques de géolocalisation se sont développées ces dernières années, utilisant des balises Bluetooth (IBeacons)[1], des bornes QR Code[2], NFC[3], UWB[4] ou des bornes utilisant les ultrasons ou la lumière (Li-Fi)[5] pour communiquer.

Le développement de ces nouvelles techniques de géolocalisation conduit donc à s'interroger sur les opportunités qu'elles offrent en termes d'usage, mais aussi sur les risques cybernétiques qu'elles apportent.

Les nouvelles techniques de géolocalisation et leurs usages

Le développement de nouvelles techniques de géolocalisation a permis de répondre à 4 types d'usages spécifiques : le géorepérage, la géolocalisation d'intérieur, la micro-localisation[6] et la géolocalisation en ligne, notamment celle issue d'HTML5.

Le géorepérage (*geofencing* en anglais)

Le « géorepérage » est le terme français retenu par la Commission générale de terminologie et de néologie comme équivalent au terme anglais « geofencing ». Il est défini comme suit : « *Détermination de la présence d'une personne ou d'un objet mobile dans une zone donnée, à partir de la géolocalisation par satellite et d'autres moyens de radiocommunication* »[7].

Le géorepérage est utilisé pour suivre l'activité d'objets ou de personnes et provoquer des réactions préprogrammées. Ce type de géolocalisation se développe sur les drones de dernière génération pour alerter leurs pilotes lorsque l'appareil s'approche ou franchit les limites d'une zone interdite de survol[8]. Il est également de plus en plus utilisé dans le marketing pour surveiller l'activité des consommateurs et envoyer des messages publicitaires ciblés par le biais d'applications mobiles[9]. A titre d'exemple, un commerçant peut mettre en place

[1] Les balises « IBeacons » sont des balises Bluetooth développées par Apple fonctionnant sur Wibree qui permettent d'envoyer un signal à un périphérique IOS à proximité et de mettre en œuvre notamment une application de géolocalisation.

[2] QR Code : Quick Response Code, code barre 2D lisible par les smartphones ou tablettes qui permet d'accéder à davantage d'information qu'un code barre conventionnel

[3] NFC : Near-field communication (communication en champ proche), technologie de communication sans contact dérivée du RFID qui permet un transfert de données limité à très faible distance, quelques centimètres seulement contre plusieurs mètres pour la RFID.

[4] L'*ultra wideband* (UWB) est une technique de modulation radio qui permet une communication sans fil de courte portée avec une large bande passante en consommant peu d'énergie.

[5] Li-Fi (*Light Fidelity*) est une technologie de communication sans-fil basée sur l'utilisation de la lumière.

[6] http://nfcom.com/geolocalisation-quelle-technologie-pour-quel-usage/

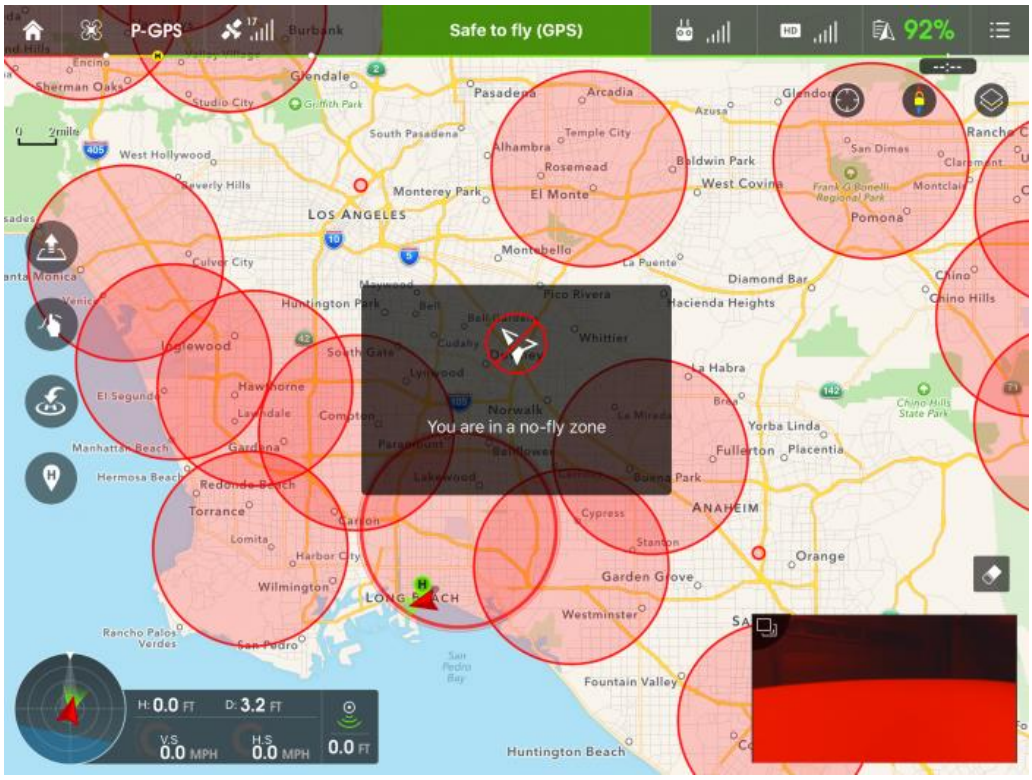
[7] https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000026461912

[8] https://www.heliguy.com/blog/2017/02/16/heliguys-guide-to-geofencing/

[9] http://www.geomarketing.com/geomarketing-101-what-is-geofencing

un dispositif de géorepérage à proximité de ses points de vente afin d'analyser le comportement des passants et leur transmettre des offres promotionnelles.

Exemple de géorepérage avec l'application DJI GO app pour drones



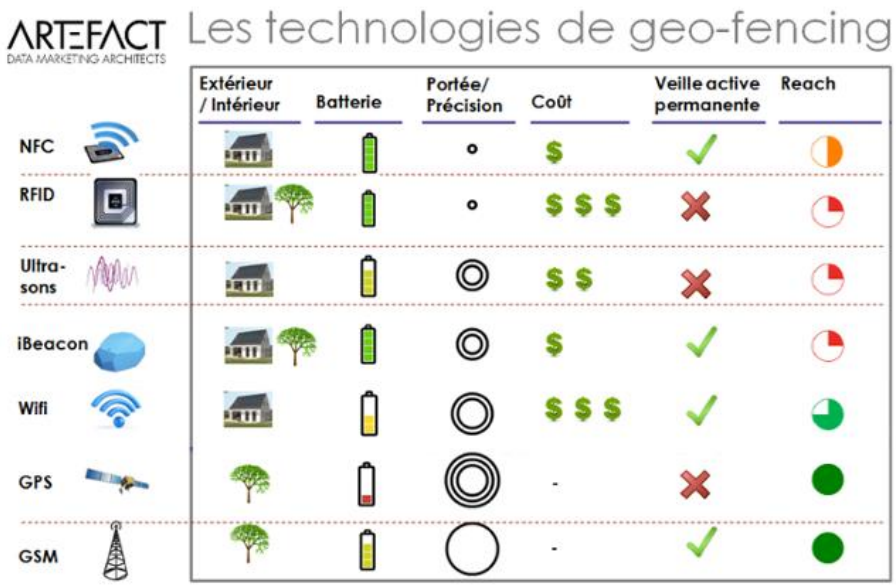
(Source : https://www.heliguy.com/blog/2017/02/16/heliguys-guide-to-geofencing/)

Dans son fonctionnement, le géorepérage consiste à créer une zone délimitée par des signaux électromagnétiques ou sonores. Les principales technologies utilisées sont ainsi :

- Les antennes relais de téléphones mobiles ;
- Les satellites dont le système GPS (*Global Positioning System*) ;
- Le Wifi ;
- Le Bluetooth ;
- Les ultrasons ;
- Le radio-identification (RFID) ;
- La communication en champ proche (NFC).

Parmi ces technologies, la NFC et le Bluetooth constitueraient les moyens techniques les plus adaptés au géorepérage. En effet, la faible portée de ces technologies permet de localiser un objet ou une personne avec précision en utilisant peu d'énergie pour un moindre coût. Notons que le Bluetooth présente également l'avantage de pouvoir être utilisé dans des environnements extérieurs et intérieurs à la différence de la NFC.

Tableau des principales technologies utilisées pour le géorepérage



Source : https://www.artefact.is/news/geolocalisation-et-media-entre-mythes-et-realites

La géolocalisation d'intérieur (géolocalisation indoor)

La géolocalisation d'intérieur (*Indoor*) est un « GPS d'intérieur » destiné aux personnes circulant dans des lieux fermés tels que des aéroports, des centres commerciaux, culturels ou sportif[10]. Elle permet de les guider à l'intérieur du lieu, d'optimiser leur visite en identifiant des points d'intérêts situés à proximité, notamment via une application telle que Google Maps Indoor[11] ou l'application « My Way Aéroports de Paris »[12]. Elle peut aussi fournir des analyses comportementales des visiteurs aux responsables du site.

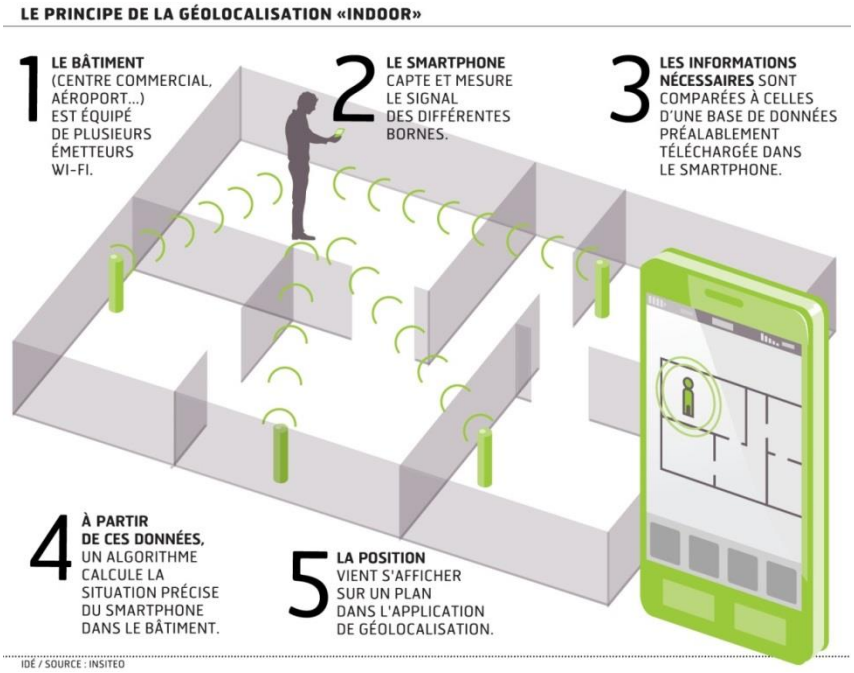
La géolocalisation d'intérieur n'est pas nouvelle. En effet, le déploiement de bornes Wifi ou Bluetooth dans les centres commerciaux ou les aéroports permet depuis longtemps de se localiser dans ces environnements.

[10] http://www.journaldunet.com/ebusiness/internet-mobile/1133686-geolocalisation-indoor-comment-ca-marche/

[11] https://www.androidcentral.com/how-use-indoor-maps-google-maps

[12] https://www.frenchweb.fr/my-way-aeroports-de-paris-application-pour-se-deplacer-dans-paris-charles-de-gaulle/18980

Exemple du fonctionnement de la géolocalisation indoor à l'aide du Wifi



(Source : Les Echos)

Toutefois, du fait de leurs limites dans les environnements intérieurs souvent complexes, les technologies Wifi et Bluetooth ne peuvent assurer une véritable géolocalisation d'intérieur en temps réel et d'une grande précision qu'en déployant de nombreuses bornes ou en combinant les solutions techniques, ce qui peut représenter un coût élevé.

Pour pallier les limites de ces technologies, une nouvelle technique consiste à utiliser l'*Ultra-Wideband* (UWB)[13]. En effet, cette technologie de transmission d'impulsions d'ondes radio de très courte durée permet de réduire les erreurs lors de la mesure du temps de propagation des signaux et ainsi de mieux calculer la position des appareils par trilatération[14], et ainsi de s'adapter aux environnements les plus complexes. Enfin, elle présente l'avantage de travailler sur une large bande de fréquences sans avoir à utiliser plusieurs antennes, ce qui permet de détecter tout type d'antenne autour du récepteur UWB tel qu'un smartphone. Soulignons que des antennes UWB se développent spécifiquement pour la géolocalisation indoor[15].

La micro-localisation

La micro-localisation est une forme de géolocalisation d'intérieur de très grande précision. Elle consiste à se localiser ou à localiser un objet ou des personnes de manière très fine afin d'interagir avec un élément spécifique (un produit sur une étagère, une œuvre d'art …). Cette forme de géolocalisation d'intérieur est

[13] https://locatify.com/blog/in-practice-precise-indoor-location-detection-with-uwb-ultra-wideband/

[14] La trilatération permet de positionner un point en utilisant la géométrie des triangles et les distances entre un minimum de deux points de référence.

[15] http://www.lembarque.com/taoglas-taille-des-antennes-uwb-specifiquement-pour-la-geolocalisation-indoor_006583

principalement utilisée dans le domaine marketing pour la publicité ciblée ou l'étude des comportements des consommateurs. Elle peut en effet reposer sur des techniques de géorepérage. La micro-localisation peut également être utilisée pour guider un consommateur vers un produit spécifique dans un magasin ou pour l'informer sur un produit. Enfin, elle peut être utilisée dans certains cas pour authentifier l'accès à un service ou à un lieu.

Le déploiement des balises Bluetooth IBeacons a contribué au développement de la micro-localisation[16]. Cependant, le développement de l'UWB devrait, comme pour la géolocalisation d'intérieur, venir renforcer la micro-localisation. Notons également que la micro-localisation se développe avec d'autres technologies telles que le QR Code.

La géolocalisation en ligne telle qu'en HTML5

Conçu pour la représentation des pages web, le format HTML5 intègre désormais une interface de programmation (API, *Application Programming Interface*) pour la géolocalisation (*Geolocation API Specification*)[17]. Ce type de géolocalisation peut être activé sur des terminaux mobiles ou fixes lors de la consultation d'une page web, permettant alors à la page web d'accéder aux coordonnées de l'utilisateur (latitude, longitude, altitude) en utilisant l'ensemble des moyens techniques dont est doté le terminal utilisé (GPS, GSM, Wifi, adresse IP, etc.). En plus des fonctionnalités traditionnelles de la géolocalisation (positionnement, orientation et indentification de points d'intérêts), il permet de trouver des résultats contextualisés sur les moteurs de recherche ou de joindre des informations géographiques à un contenu en ligne (textes/photos/vidéos). Ajoutons qu'un type de géolocalisation identique se développe sur les applications des réseaux sociaux tels que sur Facebook Messenger[18] ou Snapchat[19], notamment pour partager la localisation d'un contenu en ligne ou suggérer des nouveaux contacts. Soulignons enfin que la géolocalisation en ligne peut être également utilisée, comme le géorepérage, pour le profilage et la surveillance des utilisateurs et l'envoi de publicités ciblées.

[16] http://www.journaldunet.com/ebusiness/expert/58848/beacons--la-revolution-de-la-micro-localisation.shtml

[17] https://www.w3.org/TR/geolocation-API/

[18] https://siecledigital.fr/2017/03/28/facebook-messenger-partage-position-temps-reel/

[19] http://www.leparisien.fr/high-tech/snapchat-permet-desormais-de-geolocaliser-vos-amis-22-06-2017-7077762.php

Tableau récapitulatif des types de géolocalisation et de leurs usages

Type de géolocalisation	Technologies adaptées	Usages spécifiques
Géorepérage	• GPS • GSM • Bluetooth • Ultrasons	Déterminer la présence d'une personne ou d'un objet mobile dans une zone donnée, afin notamment de : • Surveiller l'activité d'objets ou de personnes • Alerter les utilisateurs
Géolocalisation indoor	• Wifi • UWB • Bluetooth	Se localiser dans un environnement fermé dans lesquels les signaux GPS ou GSM par exemple sont mal reçus afin notamment de : • S'orienter et trouver un itinéraire • Identifier des points d'intérêts situés à proximité (magasins, restaurants, musées, etc.).
Micro-localisation	• Bluetooth • RFID • QR Code	Se localiser précisément ou déterminer la présence de personnes ou d'objets dans un environnement spécifique et fermé afin notamment de : • Surveiller l'activité d'objets ou de personnes ; • S'orienter et d'être guidé dans un lieu spécifique ; • Alerter les utilisateurs ; • Identifier et authentifier un objet ou l'accès à un service ou un lieu
Géolocalisations en ligne de type HTML5	• GPS • GSM • Adresse IP • Wifi • Bluetooth • RFID	Se localiser ou déterminer la localisation d'une personne en ligne afin notamment de : • Se positionner et s'orienter • Identifier des points d'intérêts • Trouver des résultats contextualisés sur les moteurs de recherche • Proposer des contenus en fonction de la localisation (publicité ciblée) • Profiler et surveiller des utilisateurs • Joindre une localisation à un contenu en ligne et localiser des contacts (réseaux sociaux) • « Géoblocage » de contenu

Risques des nouvelles techniques de géolocalisation

Si les nouvelles techniques de géolocalisation offrent de nouvelles opportunités, elles peuvent présenter un risque pour le respect de la vie privée mais aussi des risques de nature cybernétique.

Le respect de la vie privée

Les nouvelles techniques de géolocalisation permettent de recueillir de nombreuses informations sur la vie privée des personnes. A ce titre, le nouveau règlement général de l'Union européenne sur la protection des données personnelles exige que certaines garanties soient accordées aux citoyens de l'Union. Un dispositif de géolocalisation doit :

- Recueillir le consentement des personnes (Opt-in) ;
- Être proportionnel et justifié pour une finalité particulière pour ne pas servir à un profilage discriminatoire ou à une surveillance illégale ;
- Permettre l'accès aux données recueillies et leur portabilité ;
- Permettre un droit d'opposition au traitement des données de localisation ;
- Permettre un « droit à l'oubli », c'est-à-dire un droit à la suppression des données de localisation.

Notons cependant que s'agissant de la collecte des points d'accès Wifi pour la constitution des bases de données de géolocalisation, il n'est pas toujours possible de recueillir le consentement des personnes. A ce titre, la CNIL a recommandé qu'il soit effectué une communication publique sur la collecte et la mise en place d'une procédure d'opposition[20]. Précisons enfin que certains smartphones Android continuent de détecter la présence de points d'accès Wifi pour optimiser la géolocalisation alors même que le Wifi est désactivé sur l'appareil[21]. Cette fonctionnalité permet ainsi la géolocalisation de l'utilisateur à son insu sans avoir à sollicité son consentement. Précisons qu'en plus de la désactivation du Wifi, il est possible de désactiver le scanner Wifi dans les réglages du smartphone ou de passer en mode avion lorsque la désactivation du scanner Wifi n'est pas prévue comme dans le cas du Smartphone OnePlus One.

Risques contre les systèmes de géolocalisation

Différentes attaques peuvent être dirigées contre les systèmes de géolocalisation. Elles peuvent servir à :

- Empêcher la géolocalisation (brouillage des réseaux sans fil ou attaque de type DDoS) ;
- Détourner la géolocalisation (variation de la puissance d'émission du signal afin d'altérer le calcul des distances ou modification de l'adresse MAC pour ne pas être identifié[22]) ;
- Accéder à des données de géolocalisation (piratage des sites web utilisant l'API de géolocalisation[23] ou plus généralement des bases de données de géolocalisation).

Ces risques pour les systèmes de géolocalisation peuvent entraîner de nombreuses conséquences néfastes dans leurs usages. On peut ainsi imaginer le détournement d'un drone ou de son dispositif d'alerte lorsqu'il utilise le geofencing. De même, il serait possible d'empêcher ou d'usurper l'authentification d'un utilisateur lorsqu'il s'appuie sur la micro-localisation.

Piratage et prise de contrôle des infrastructures réseaux et des appareils connectés

Le déploiement de dispositifs permettant la géolocalisation présente des risques pour les infrastructures réseaux et les appareils qui y sont connectés. En effet, ces dispositifs s'appuient sur les objets connectés alors que la sécurité de ces appareils n'est pas pleinement assurée, notamment en raison de vulnérabilités qui ne peuvent pas obtenir de mise à jour. En outre, ils renforcent également la connectivité entre les appareils dans des environnements publics (gares, aéroports, centres commerciaux, etc.). A ce titre, les connexions Bluetooth ou Wifi peuvent être exploité par des acteurs malveillants pour infecter les infrastructures réseaux et les appareils des utilisateurs. Par exemple, la vulnérabilité BlueBorne permet

[20] http://www.netpublic.fr/2012/01/geolocalisation-et-points-d-acces-wifi/

[21] http://www.01net.com/actualites/sur-android-le-wi-fi-peut-vous-tracer-meme-s-il-est-desactive-1245292.html

[22] L'adresse MAC (Media Access Control) est un identifiant physique de carte réseau ou d'une interface réseau similaire. Si elle est unique, elle peut être modifiée numériquement en créant une nouvelle adresse MAC ou en utilisant l'adresse MAC d'un autre appareil.

[23] https://www.developpez.com/actu/98354/L-API-de-geolocalisation-ne-sera-plus-accessible-pour-des-contextes-non-securises-a-partir-de-Chrome-50-afin-de-mieux-proteger-ce-type-de-donnees/

l'exécution de code malveillant sur une machine ciblée ou une attaque de type man-in-the-middle pour intercepter le trafic lorsque le Bluetooth est activé[24]. Il en va de même pour la connexion Wifi avec la récente découverte de vulnérabilités affectant le protocole WPA2[25]. Par ailleurs, le développement d'autres technologies pour la géolocalisation telles que l'ultrason devraient venir élargir la surface d'attaque[26].

Conclusion

Les nouvelles techniques de géolocalisation ouvrent de nouvelles perspectives. Elles permettent de compléter les systèmes de positionnement par satellites et de contribuer ainsi au développement des programmes de type ASPN (*All Source Positioning and Navigation*) [27]. Elles promettent une généralisation de la géolocalisation, ce qui va entraîner la multiplication d'opérateurs traitant des données de géolocalisation (commerces, plateformes en ligne, utilisateurs finaux, etc.). Cette prolifération d'opérateurs utilisant la géolocalisation pourrait accompagner le travail des forces de sécurité, notamment en matière de lutte contre le terrorisme ou la criminalité organisée. Toutefois, il n'est pas impossible que des opérateurs refusent ou rendent difficile l'accès à ses données afin de protéger leurs intérêts en privilégiant la confidentialité des données de leurs clients par exemple.

[24] http://www.zdnet.fr/actualites/blueborne-de-multiples-failles-dans-le-bluetooth-inquietent-les-fabricants-39857236.htm

[25] https://arstechnica.com/information-technology/2017/10/severe-flaw-in-wpa2-protocol-leaves-wi-fi-traffic-open-to-eavesdropping/

[26] http://www.journaldunet.com/solutions/expert/58464/la-communication-ultrasonique---une-revolution-silencieuse.shtml

[27] http://www.militaryaerospace.com/articles/2013/02/SAIC-DARPA-ASPN.html

PORTEE ET LIMITES DU BROUILLARD CYBERNETIQUE

Vous êtes au beau milieu d'une forêt. Impossible de voir au-delà des arbres. Soudain, une pierre tombe et vous blesse. Vous savez que cette pierre a dû être ramassée du sol, puis jetée. Mais vous ne pouvez pas savoir d'où vient la pierre, ni qui a fait le coup. Vous savez juste que certains acteurs ont installé leur camp dans les environs, le problème étant que d'autres qui se promènent souvent dans le coin auraient très bien pu ramasser la pierre et la lancer. Par ailleurs, vous ne savez pas si d'autres attaques vont être lancées, si vous avez été ciblé, et si oui, la raison pour laquelle vous l'avez été. Vous êtes alors devant un choix : vous protéger ? Renvoyer la pierre dans la direction qui vous semble la plus vraisemblable ? Dénoncer publiquement celui que vous pensez être à l'origine de l'attaque ? Le tout sans avoir eu le temps de mener des investigations quant à la composition de la pierre et à son origine possible, à l'endroit d'où elle a pu être lancée et aux motivations qui auraient pu pousser certains à vous attaquer.

Prenons maintenant la situation de l'autre côté. Vous souhaitez troubler votre voisin dans la forêt. Vous pouvez jeter une pierre de votre camp, et espérer que l'attaque intimide suffisamment votre adversaire. Mais celui-ci pourra au bout d'un moment identifier l'origine de la pierre et, s'il choisit de riposter, les représailles pourront être dommageables pour vous. Bien sûr, vous pouvez nier avoir jeté la pierre, ce qui pourra tenir pour un moment. Mais vous avez aussi la possibilité de profiter de l'épaisseur de la forêt pour éviter tout problème en prenant une pierre dans un autre lieu. Vous pouvez aussi la lancer d'un autre endroit, voire vous placer à proximité d'un autre camp pour faire accuser quelqu'un d'autre. Vous pouvez enfin écrire un message sur la pierre pour déstabiliser votre adversaire et ajouter à la confusion ambiante en émettant de fausses revendications. Votre intérêt : pousser deux adversaires à se battre entre eux.

Le cyberespace est à l'image de cette épaisse forêt, les malwares pouvant être comparés aux pierres lancées par les différents occupants de la forêt qui peuvent tous attaquer mais sont également tous vulnérables. Les noms y sont pseudonymes, la géographie y est floue et les motivations y sont ambivalentes. C'est donc un monde de déduction et de traces (techniques, tactiques et procédures, ou TTPs) dont peuvent disposer les groupes les plus puissants, mais où le doute règne. Les identités n'y sont pas figées : un groupe peut être identifié, mais ses alliances et affiliations ne le seront peut-être jamais.

L'utilisation du brouillard cybernétique dans les opérations offensives

En l'absence de repères géographiques, le cyberespace n'offre pas à son utilisateur de visibilité directe sur son environnement. Le brouillard, que son architecture technique, sa complexité technologique et ses modèles économiques autorisent, voire favorisent, offre un fort avantage aux stratégies offensives. L'anonymat et le climat d'incertitude qui en résultent procurent en effet une grande liberté d'action et de manœuvre pour des acteurs souhaitant rester « sous le radar ». Ceux-ci pourront notamment se camoufler en exploitant des dynamiques politico-diplomatiques existantes, voire tromper sciemment un adversaire en se faire passer pour d'autres.

L'exploitation des dynamiques politico-diplomatiques existantes

L'attaquant peut tout d'abord profiter des tensions et dynamiques existantes pour réaliser une opération. Dans le cas où des tensions existent déjà entre deux ou plusieurs Etats, l'objectif est de détourner l'attention et de faire attribuer l'opération, une fois celle-ci détectée, à l'un ou l'autre des Etats impliqués dans ces tensions. L'auteur de l'attaque peut ainsi espérer dans un premier temps échapper aux accusations, à charge pour lui de rendre toute accusation impossible en maintenant le doute dans la durée. Autre situation : un incident cybernétique a déjà éclaté et un coupable est désigné. Même s'il en résultera sans doute un renforcement momentané de la surveillance des réseaux, cette situation offrira de nombreuses opportunités pour un attaquant sur d'autres cibles au sein du même pays, car la focalisation sur un coupable supposé lui permettra de passer inaperçu. Et si l'attaque est détectée, elle sera rapidement attribuée au coupable déjà identifié.

Autant de situations qui se sont déjà produites. Lors de l'attaque visant le Parlement britannique en juin 2017, un groupe des pirates russes est par exemple accusé d'avoir récupéré des mots de passe de parlementaires, de membre du cabinet et d'ambassadeurs.[28] Une semaine après, une autre attaque cybernétique sur le Parlement britannique est détectée. Les Russes sont de nouveau accusés.[29] Alors que l'investigation n'en n'est qu'à ses débuts, c'est même le Gouvernement russe qui est explicitement accusé. Peu importe à ce stade les données techniques, les attaques déjà subies et le climat de tension entre les deux pays suffit à les faire accuser. Pourtant 4 mois après, alors que Donald Trump prend position contre l'accord nucléaire avec l'Iran[30], les accusations changent : ce n'est plus la Russie qui est montrée du doigt mais l'Iran. Compte tenu de la difficulté d'obtenir rapidement des éléments techniques probants et de l'impossibilité d'en faire état publiquement lorsque l'on en dispose, les tensions diplomatiques influent donc lourdement sur l'attribution des attaques.

Autre exemple : le groupe Shadow Brokers, qui affirme être en possession des outils d'attaque de la *National Security Agency* (NSA). Dans un climat déjà tendu après les soupçons de piratage et d'ingérence dans les élections présidentielles américaines, les médias ont rapidement désigné la Russie comme étant derrière le groupe[31]. Un climat vraisemblablement exploité par le groupe Shadow Brokers, qui a profité de cette communication sur leurs opérations pour semer la confusion[32]. Pendant que la communauté des chercheurs cherchait à attribuer les actions du groupe à un pays, les Shadow Brokers ont ainsi joué avec les hypothèses émises en diffusant nombre d'informations non vérifiables destinées à créer le doute. Ils ont ainsi diffusé des messages affirmant qu'ils résidaient aux Etats Unis. Ils ont également indiqué que leur écriture en faux mauvais anglais était une tactique visant à déjouer les investigations et qu'ils appartenaient la NSA avant de décider de se retourner contre leur gouvernement pour combattre les injustices qu'ils voyaient. Ils se sont enfin exprimés sur tous les sujets d'actualité, avec une connaissance des références culturelles américaines qui

---

[28] Goddard, Louis, « Ministers' email addresses and passwords up for sale », *The Times*, June 23 2017. Web: https://www.thetimes.co.uk/edition/news/russian-hackers-trade-british-ministers-email-addresses-and-passwords-hqtr7pv9z

[29] MacAskill, Ewan, and Rajeev Syal, « Cyber-attack on UK parliament: Russia is suspected culprit", *The Guardian*, 25 June 2017. Web: https://www.theguardian.com/politics/2017/jun/25/cyber-attack-on-uk-parliament-russia-is-suspected-culprit

[30] MacAskill, Ewen, « Iran to blame for cyber-attack on MPs' emails – British Intelligence », *The Guardian*, 14 October 2017.

[31] Schneier, Brice, « Who are the Shadow Brokers? », *The Atlantic*, 23 May 2017. Voir aussi des reportages de CNN. Comme celui-ci: Patterson, Thom, "The Russian spies living next door", *CNN*, 19 July, 2017. Web: http://edition.cnn.com/2017/07/19/us/russian-spies-united-states-declassified/index.html

[32] @x0rz, « Shadow Brokers : Courtier ou agent d'influence ? » *MISC*, N. 93, septembre/octobre 2013.

pouvait corroborer leur possible origine américaine. Tout cela a finalement contribué à la difficulté d'une attribution claire pour le grand public et à l'impossibilité pour le gouvernement des Etats Unis de montrer du doigt rapidement un pays. Bref, de quoi permettre aux attaquants de gagner du temps.

Pour un attaquant, un conflit diplomatique préexistant peut donc être exploité pour semer le doute quant à l'origine d'une opération cybernétique détectée. On parlera alors de manœuvre diplomatique dans un contexte cybernétique, à ne pas confondre avec la manœuvre cybernétique dans un contexte militaire. Dans cette deuxième situation, c'est l'opération cybernétique elle-même qui aura pour objectif de diriger l'attention de l'adversaire vers une région spécifique et de le détourner d'une autre. Une opération informatique contre le réseau électrique dans une partie d'un pays pourra par exemple laisser penser que l'attaque conventionnelle aura lieu dans la région affectée alors qu'elle se déroulera dans une autre.

La « fourth-party collection »

Si les attaquants peuvent camoufler leurs opérations derrière les tensions préexistantes et profiter du brouillard généré par les biais cognitifs que ces tensions peuvent développer, ils peuvent également sciemment induire en erreur leurs adversaires. Les traces techniques laissées lors d'une opération, de même que les outils d'attaque développés et non encore utilisés, offrent en effet de nouvelles opportunités de manipulation. Dans le cadre d'opérations de « fourth party collection », les services de renseignement peuvent ainsi pirater des groupes qui ont eux-mêmes piraté d'autres groupes, non seulement pour voler les informations qu'ils ont récupéré mais également pour s'emparer de leurs outils et de leurs infrastructures et perpétrer des attaques en leur nom[33]. La victime peut être un groupe cybercriminel, un service de renseignement domestique, voire même un service de renseignement étranger moins puissants. C'est de cette manière que les TTPs trouvés lors d'une investigation peuvent être trompeurs et porter la marque d'un groupe qui a lui-même été piraté par le véritable auteur de l'opération. Si l'anonymat bénéficie au « faible », il peut aussi profiter au « puissant » qui dispose des capacités technologiques requises.

Israël a ainsi récemment révélé que la Russie avait pu accéder à des données de la NSA au travers de l'antivirus de Kaspersky Labs en accédant à l'ordinateur personnel d'un agent de la NSA qui en était équipé et qui stockait, au mépris de toutes les règles de sécurité, des données confidentielles sur son ordinateur personnel[34]. Des opérations ont donc pu théoriquement être montées avec des outils de la NSA sans que les Etats-Unis y soient impliqués.

Ce dernier type d'opération laissera cependant des traces, à l'image de celles identifiées par les chercheurs de Kaspersky pendant leurs investigations sur des groupes comme Crouching Yeti, DarkHotel et NetTraveler. Différents éléments (présence de *backdoors* et de divers artefacts) indiquaient la présence d'autres entités au sein de l'infrastructure mis en place par les attaquants. De quoi indiquer non seulement que des données avaient été volées mais que des exploits, des outils et des codes source avaient sans doute pu être réutilisés ou intégrés à d'autres kits d'attaque, rendant ainsi impossible toute attribution future. Autre exemple présenté

[33] Guerrero-Saade, Juan Andres and Raiu, Costin, « Walking in your Enemy's Shadow: When Fourth-Party Collection Becomes Attribution Hell" *Kaspersky Lab, USA & Romania*, Virus Bulletin Conference October 2017.

[34] Nakashima, Ellen, « Israel hacked Kaspersky, then tipped the NSA that its tools had been breached », *The Washington Post*, 10 October 2017. Web: https://www.washingtonpost.com/world/national-security/israel-hacked-kaspersky-then-tipped-the-nsa-that-its-tools-had-been-breached/2017/10/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html

par Kaspersky : le groupe APT baptisé Dancing Salome qui a réutilisé les outils de HackingTeam et ses fameux *Remote Control Systems*.[35]

Quelle défense face au brouillard des opérations cybernétiques ?

Les opérations cybernétiques offensives ont des effets qui dépassent l'impact direct de l'opération sur les données ou sur le système visé. La cible voit en effet sa marge de manœuvre réduite par les effets psychologiques produits par les opérations cybernétiques et le fait que des postures purement dissuasives ne fonctionnent pas. La plupart du temps, la crainte de ses propres vulnérabilités et la difficulté de l'attribution empêchent ainsi le défenseur de riposter. Celui-ci se retrouve alors soumis à des pressions politiques et contraint de choisir, par un raisonnement politique, un bouc-émissaire tout désigné. Cette asymétrie entre l'attaque et la défense en matière cyber est cependant largement exagérée, l'obsession de l'attribution étant au cœur de ce déséquilibre.

Les effets psychologiques des opérations cyber

La difficulté essentielle de la défense cybernétique réside dans la focalisation sur la problématique de l'attribution après chaque incident. A l'instar de ce qui s'est passé lors de l'attaque contre le Parlement britannique ou des fuites du groupe Shadow Brokers, la presse et l'ensemble des observateurs cherchent aussitôt à « attribuer » l'attaque, tandis que les autorités se retrouvent contraintes de prendre rapidement position sur la « possible origine » des attaquants. C'est cette volonté de relier la dimension cybernétique à la dimension géographique qui est à la source de tous les effets psychologiques des opérations hybrides, et qui est donc en quelque sorte le défaut originel de la défense cybernétique.

En cas d'attaque, les premières questions que se poseront en effet les défenseurs seront : qui est le vrai auteur de l'attaque ? Qu'est-ce que je dois protéger et contre qui ? Autant de questions qui déstabilisent le défenseur et génèrent une véritable escalade. Le défenseur doit agir comme s'il était certain d'être piraté et partir de la supposition que les systèmes ne sont pas sûrs[36] et qu'ils seront pénétrés un jour ou l'autre. Il doit également prioriser et décider des informations à exposer et des informations à protéger. L'ombre des opérations cybernétiques plane ainsi dès le départ sur le défenseur… Autre défi : pour un Etat respectueux du droit international, la riposte sera nécessairement plus difficile compte tenu de la difficulté technique de l'attribution et des règles juridique entourant la légitime défense. Les aspects juridiques se doublent enfin de réelles difficultés techniques quant à la planification et l'exécution d'opérations d'attaques informatiques ciblées. Nombre d'opérations cybernétiques planifiées en accompagnement d'opérations militaires, comme en Irak en 2003, ont ainsi été annulées en raison de l'impossibilité de garantir que les effets de l'attaque allaient rester circonscrits aux systèmes visés. Autre exemple plus récent de la « peur cybernétique » qui touche les défenseurs : l'ancien *Director for National Intelligence* (DNI) aux Etats Unis, James Clapper, déclarait en 2012 que le pays n'avait pas voulu riposter après les attaques en déni de service sur les banques américaines par crainte de ne pas être capables de défendre l'infrastructure digital du pays contre de possibles contre-attaques

[35] Guerrero-Saade, Juan Andres and Raiu, Costin, « Walking in your Enemy's Shadow: When Fourth-Party Collection Becomes Attribution Hell" *Kaspersky Lab, USA & Romania*, Virus Bulletin Conference October 2017

[36] Ducaru, Sorin, « Is Cyber Defense Possible ? » *Journal of International Affairs*, Winter 2013 ; 70, 1 ; ProQuest pg. 182.

qui ne seraient pas « précises et légalistes ».[37] La dissuasion jouait donc en faveur de l'attaquant et non du défenseur !Autant de difficultés qui affaiblissent clairement la posture du défenseur cybernétique et font que la dissuasion dans le cyberespace se situe davantage dans les registres militaire et diplomatique que dans le domaine cybernétique.

Pour compenser cette faiblesse, les Etats tentent aujourd'hui de mettre en place des mécanismes d'autorégulation sur la base de « comportements responsables ». Et quand ils échouent dans leurs négociations comme lors de la dernière réunion du Groupe gouvernemental d'experts (GGE) à l'ONU, c'est une entreprise, Microsoft, qui appelle les Etats à signer une « convention de Genève » du numérique[38]. De quoi accréditer la thèse, simple mais trompeuse, que le cyberespace est devenu l'un des lieux d'affrontement préféré des Etats en situation de paix, au détriment du secteur privé.

Les avantages de la défense cybernétique

Même si le brouillard qui entoure les opérations cybernétiques est un avantage non négligeable, en particulier pour les opérations psychologiques et de renseignement, les opérations offensives possèdent leurs propres limites, ne serait-ce que parce qu'elles ne permettent pas, de façon autonome, de contrôler un territoire[39].

La posture de défense cybernétique possède également des avantages à faire valoir face à l'attaque. Comme pour toute posture de défense efficace, cela suppose tout d'abord que le défenseur se pose les bonnes questions en se mettant dans la peau de l'attaquant : quelles sont mes cibles prioritaires ? Qu'est-ce que les défenseurs s'attendent à voir attaquer en priorité ? Quels sont les modes opératoires que je vais utiliser ? Autant de questions qui permettront d'identifier les menaces potentielles, d'analyser les modes opératoires, et de prendre les mesures nécessaires en termes d'anticipation, de protection, de détection et de réaction.

Parmi les avantages de poids dont dispose la défense : les traces laissées par les attaquants. Même si celles-ci sont peu fiables en termes d'attribution compte tenu des stratégies de « fourth parties », elles peuvent être utilisées de plus en plus efficacement pour améliorer ses capacités de détection, grâce notamment aux progrès de l'intelligence artificielle. Les technologies deviennent ainsi de plus en plus compétitives[40]. L'asymétrie attaque/défense en termes de coût doit en outre être relativisée en termes de coût : les attaques sophistiquées, par exemple contre des systèmes industriels, requièrent en effet des moyens importants. Développer une arme informatique suppose du temps et des compétences. Il faut ensuite du renseignement opérationnel, de l'information sur les réseaux et l'infrastructure ciblée, des connaissances sur les modalités d'accès et les accès eux-mêmes. Et sa durée de vie opérationnelle est limitée puisqu'elle devient généralement obsolète dès qu'elle a été utilisée et surtout détectée.

---

[37] Waterman, Shaun, « Clapper : U.S. shelved « hack backs » due to counterattack fears », *Cyberscoop*, 2 October 2017.

[38] Smith, Brad, « Growing Consensus on the need for an International Treaty on Nation-State Attacks », *Microsoft Blogs*, 13 April 2017, Web: https://blogs.microsoft.com/on-the-issues/2017/04/13/growing-consensus-need-international-treaty-nation-state-attacks/

[39] Gartzke, Erik « The myth of cyber war: Bringing War on the Internet Back Down to Earth », *University of California San Diego*, 7 December 2012.

[40] Rid, Thomas, *Cyber War will not Take Place*, Oxford University Press, 2013.

Cinq facteurs permettent de déterminer l'intérêt relatif des opérations cybernétiques, qu'elles soient de nature offensive ou défensive[41] :

- L'économie de l'armement cyber est très différente de celle de l'armement conventionnel en raison du lien indissociable existant entre les compétences et la créativité individuelles des personnes qui développent ses capacités et les technologies elles-mêmes. Impossible d'imaginer, par exemple, des chaines de production d'armements cybernétiques ;
- Le coût des opérations cybernétiques pour une organisation dépend de la complexité des technologies requises et de la maturité technologique de l'organisation considérée ;
- Le coût relativement important des opérations défensives provient de la complexité de cette posture. Lorsque les opérations offensives deviennent elles-mêmes plus complexes, leur coût augmente également ;
- Les avantages que la complexité de l'espace numérique procure à l'approche offensive s'arrêtent avec les limites de cet espace, c'est à dire là où les systèmes numériques rencontrent les équipements physiques ;
- La valeur des opérations cybernétiques doit être considérée à l'aune des objectifs politiques des adversaires.

Ces facteurs ne sont pas des variables dissociables. L'intérêt relatif du défensif ou de l'offensif n'est en réalité pas lié à la nature même du cyberespace : il dépend de chaque situation et des parties au conflit. De plus, les technologies développées pour les opérations offensives ne présentent d'intérêt que si la cible dispose de vulnérabilités liées aux technologies de l'information. Elles ne permettent pas, à elles seules, de contrôler physiquement un territoire. La question est donc de savoir si leur principal intérêt ne concerne pas uniquement les opérations psychologiques et le renseignement. Par ailleurs, leur avantage supposé n'apparaît pas lié aux aspects technologiques mais à la mauvaise gestion de la défense et aux limites fixées aux opérations offensives qui entravent les capacités de réponse[42]. La technologie ne peut donc pas être la source de l'avantage, d'autant qu'une fois détectée, l'arme cybernétique devient obsolète. Ce sont les compétences techniques et la capacité à produire en permanence de nouvelles armes qui fondent avant tout autre chose la puissance cybernétique au plan offensif. Même constat pour la posture de défense : les compétences, la capacité de détection, la réactivité des opérateurs et l'hygiène informatiques déterminent son efficacité.

Qu'il s'agisse d'attaque ou de défense, le défi des organisations réside dans la complexité de la technologie informatique. Plus il y a de complexité, plus il y a de vulnérabilités. Même si cet avantage doit être relativisé avec le développement des « organisations étendues » et la pratique croissante du *shadow IT*, la défense a cependant l'avantage du terrain, pour peu qu'elle se donne la peine de le maitriser. Les organisations dotées d'excellents processus de gestion des risques numériques réduisent ainsi considérablement l'avantage des postures offensives. L'échange d'information sur les menaces entre organisations est également crucial, puisque la vitesse de détection des cyberattaques les plus sophistiquées en dépend. L'avantage que l'on

[41] Slayton, Rebecca, « What is the Cyber Offense-Defense Balance ? Conceptions, Causes, and Assessment », *International Security*, Vol. 41, No 3 (Winter 2016/17) pp. 72-109 .

[42] Slayton, Rebecca, « What is the Cyber Offense-Defense Balance ? Conceptions, Causes, and Assessment », *International Security*, Vol. 41, No 3 (Winter 2016/17) pp. 72-109.

accorde ainsi souvent à l'attaque sur la défense en matière cybernétique repose donc largement sur la défaillance des organisations en matière de défense.

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.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la Défense
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.eu