Les objets connectés dans les missions judiciaires

Par **François BOUCHAUD**
Capitaine de gendarmerie, Centre de lutte contre les criminalités numériques (C3N) au sein du Commandement de la gendarmerie dans le cyberespace (ComCyberGend)
Et **Thomas VANTROYS**
Maître de conférences à l'Université de Lille et membre du laboratoire CRIStAL (UMR 9189) et de l'IRCICA (USR 3380)

La généralisation des technologies de l'information interactives dans le quotidien constitue, avec la prolifération des objets intelligents communicants, un enjeu d'actualité dans le cadre des missions judiciaires. Peu visibles, à l'exception des plus populaires d'entre eux comme, entre autres, les montres connectées, ces derniers s'invitent et participent à notre quotidien. Tous les secteurs d'activité sont touchés par cette numérisation accélérée. L'Internet des objets, IdO (en anglais, IoT), suscite aujourd'hui autant de promesses d'opportunités économiques, sociétales et judiciaires que de questions, voire d'inquiétudes, certaines de portée stratégique. Dans cet article, nous exposons les opportunités offertes par les objets connectés dans le cadre des missions judiciaires. Nous nous intéressons également à quelques-unes des nouvelles menaces liées à l'usage et au déploiement de ces écosystèmes.

Les objets connectés, de nouvelles opportunités pour les forces de sécurité

La révolution de l'IdO permet aux objets de la vie quotidienne d'intégrer une multitude de capteurs et d'actionneurs. La multiplication et la massification de ces équipements entraînent une numérisation du réel. Le numérique se superpose et interagit avec le monde physique. Les objets connectés scrutent et interfèrent avec notre quotidien. Ils génèrent une grande diversité d'informations : des données d'utilisateurs, de contexte, de système, des logs de fonctionnement, etc. L'accroissement des objets déployés amène à un volume total d'informations échangées extrêmement élevé. Les données collectées constituent une nouvelle manne économique. Elles sont l'« or noir » du XXI^{e} siècle. Ainsi, tous les deux ans, la volumétrie des données générées par l'Internet des objets double la taille de l'univers numérique, il est estimé en 2020 à 44 000 milliards de giga-octets (Cosquer, 2016). L'horizon de l'Internet des objets dans un écosystème numérique, désormais global, ouvre à d'importants enjeux et à des promesses d'opportunités pour le renseignement, la conduite opérationnelle, l'investigation judiciaire et la défense. Ces données participent également à l'innovation dans la création de services personnalisés, en réponse aux besoins actuels et futurs. Ainsi, ce phénomène bouleverse les frontières traditionnelles. Il révolutionne les chaînes de valeur de l'entreprise et l'organisation territoriale. La limite entre le virtuel et le réel est en passe d'être abolie. Elle s'inscrit dans une logique de *continuum* cyberespace-espace physique (Hazane, 2018).

Les objets connectés inscrits dans l'infrastructure de l'IdO créent une donnée longitudinale qui propose non seulement de pouvoir identifier et de fournir tous les éléments matériels nécessaires à la manifestation de la vérité judiciaire, mais offre également des champs à la prévention et à

l'analyse des phénomènes. Le croisement des traces autorise des recoupements d'informations et des investigations inédites. La presse internationale se fait l'écho de plusieurs enquêtes criminelles incorporant des écosystèmes connectés. Des enquêteurs du Merseyside (Royaume-Uni) ont exploité les logs de fonctionnement et les données de géolocalisation d'une montre sportive GPS dans la résolution de l'affaire Paul Massey (Thomas, 2019). Les informations recueillies ont permis de reconstruire la chronologie des évènements survenus et de qualifier l'infraction en mettant en avant une préméditation du fait criminel. En Arkansas (États-Unis), l'appareil Amazon Echo a servi de témoin dans un meurtre en enregistrant les bruits ambiants (Chavez, 2017). Dans l'affaire Anthony Aiello en Californie (États-Unis), la correspondance entre les données du bracelet connecté de la victime et les informations du système domotique a permis de confondre le meurtrier en contextualisant le crime (Cassidy, 2018). L'objet connecté détourné de son usage premier offre des informations inédites pour l'investigation judiciaire. C'est notamment le cas des thermostats connectés disposant de facultés d'apprentissage. Couplés à l'écosystème de la maison, ces équipements sont en mesure de déclencher des actions automatiques tel l'allumage du chauffage lorsque le téléphone est reconnu dans un champ proche. Cette information est exploitable pour reconstituer la chronologie des événements révolus, et déterminer des présences ou des déplacements dans un périmètre donné. L'objet connecté est la face visible et locale de l'infrastructure de l'Internet des objets, porte d'entrée des investigations judiciaires. La recherche, l'identification et l'analyse de cet élément catalyseur sont primordiales pour comprendre l'architecture globale et obtenir une information pertinente au regard de l'enquête. L'enquêteur doit être en mesure d'associer à un phénomène criminel et sa donnée, un dispositif physique. Il doit ainsi comprendre le parcours de l'information dans l'architecture connectée, de son initialisation à son interception. Cette perception oriente les investigations et les actes techniques dans l'obtention de preuves pour le procès pénal. La valeur ajoutée de l'Internet des objets vient du fait que le tout est plus grand que la somme des parties, ce qui explique que les approches unité par unité passent à côté de la valeur ajoutée de l'IdO (Bouchaud, 2021).

L'identification des objets et leur caractérisation technique sont la clef de voûte pour l'extraction et l'étude de l'information pertinente. Or, la diversité d'usage, de fonctionnement dans la remontée et la synchronisation de l'information, l'hétérogénéité des objets interdépendants rendent jusqu'à présent ce travail d'investigation très chronophage et fastidieux en l'absence d'une approche intégrale d'analyse. Parcellaire dans un objet, la donnée prend son sens dans l'architecture globale. Comment appréhender avec intelligence les objets et leur environnement de connexion dans un contexte judiciaire ? Comment accéder à ce gisement d'information eu égard aux nombreuses dépendances, aux liens cachés, à sa dispersion et à sa fragmentation dans l'infrastructure connectée ? Quelle crédibilité donner aux traces recueillies et reconstruites ? Sont-elles fiables et robustes pour l'enquête, et donc présentables devant une cour de justice ?

L'interception des données sensibles par l'exploitation des failles de sécurité des appareils connectés et des données systèmes s'avère primordiale pour l'investigation. L'authentification des agents communicants, l'exploitation et la contextualisation des données à des fins d'analyse, le croisement entre les informations recueillies, le contrôle de l'exposition des données nécessitent en effet une amélioration continue des techniques d'expertise. Pour l'investigation judiciaire, il s'agit d'anticiper l'apparition de nouvelles formes de criminalité, de gagner en agilité et en fiabilité, et dès lors répondre à la demande croissante d'expertise. L'objectif est également de limiter les usages impropres qui pourraient être faits à partir des données. L'expert criminel en nouvelles technologies doit s'assurer du maintien de l'intégrité et de la qualité des données, de la collecte des éléments matériels pertinents à leur présentation devant une cour de justice. Or, la collecte des données se heurte à plusieurs difficultés : ces données numériques sont souvent dispersées et rendues anonymes, contraintes par des politiques propres de gestion. Leurs manipulations à des fins d'exploitation ou de conservation s'avèrent difficiles et les rendent sujettes à de potentielles

altérations. Il est de plus essentiel de réaliser le chaînage des données pour obtenir une lecture de l'information lisible.

Ce constat est également applicable à la collecte d'information dans le cadre du renseignement. Un rapport publié le 1er février 2016 par le centre de recherche Berkman de l'université Harvard (Gasser, 2016) estime que la quantité de données rassemblées par les objets connectés en fait l'une des pistes privilégiées pour que les agences de renseignement puissent contourner les protections mises en place sur les moyens de communication « classiques ». En 2016, James Clapper, directeur du renseignement national des États-Unis, a déclaré lors d'une audition devant le Sénat américain : « À l'avenir, les services de renseignements pourraient tirer parti de l'Internet des objets pour identifier, surveiller ou localiser des suspects, découvrir des indicateurs potentiels, ou obtenir des mots de passe » (*Le Monde*, 2016).

Une nouvelle source de menaces à l'échelle internationale

Une nouvelle porte d'entrée dans les systèmes d'information

L'utilisation croissante des objets connectés a de fortes implications en matière de sécurité et de confidentialité des données échangées. Les dispositifs détournés par malveillance de leurs usages premiers introduisent de nouveaux risques, des menaces d'atteintes numériques et économiques. Le cas récent d'un vol de données provenant du système d'information d'un casino aux États-Unis, passant par un thermomètre connecté d'aquarium, illustre ce phénomène grandissant (Williams-Grut, 2018). L'environnement connecté se transforme en un vecteur criminel : de façon accessoire en facilitant la commission d'une infraction, de manière principale lorsqu'elle se rapporte au contenu ou bien en constituant son objet. Concrètement, cette singularité cybercriminelle se traduit de plusieurs manières : par des perturbations du fonctionnement nominal d'un dispositif connecté en l'empêchant de transmettre des données, par la prise de contrôle logique ou physique de l'environnement connecté en le détournant de son usage premier, et/ou par un accès illégal aux informations échangées ou stockées en portant atteinte aux données personnelles. Pour les entreprises, il s'agit de préserver la confiance des clients en garantissant la confidentialité des données personnelles, la sécurité des transactions, la protection à l'égard des logiciels malveillants et des attaques informatiques.

À ces risques identifiés s'ajoutent la maîtrise et la supervision d'un parc d'objets en cohérence avec les habitudes et les usages de consommateurs de services. En effet, la facilité de déploiement et d'utilisation des objets connectés devient un nouveau défi pour les administrateurs des systèmes et des réseaux d'entreprise. Un déploiement anarchique de solutions par des salariés occasionne des perturbations des réseaux existants. La question de la détection et de l'identification des objets connectés devient donc un élément central pour garantir la sécurité des systèmes d'information.

Par ailleurs, la mise en péril de la santé publique ou d'un écosystème est également réelle s'agissant d'appareils dont l'utilisation a un lien direct avec la santé ou la sécurité. Ces menaces sont amplifiées par la diffusion et la massification accélérées de dispositifs composites dans un écosystème anarchique non régulé et non réglementé. Cet environnement informatique souffre d'une insuffisance de vision globale en matière de sécurité (*security by design*). Une récente étude de la société Palo Alto Networks révèle ainsi que 98 % du trafic des objets connectés utilisés dans un environnement professionnel ne sont pas chiffrés et 57 % d'entre eux comprendraient des vulnérabilités (Unit 42, 2020), générant un risque systémique préfiguré par le *botnet* Mirai (2016). En effet, l'absence de standards de sécurité, l'hétérogénéité des protocoles et des technologies utilisés, le manque de bonnes pratiques en matière de conception, notamment dans le maintien en condition de sécurité ou la mise à jour des *firmwares* des objets déjà déployés génèrent des risques élevés. Ainsi, les objets connectés sont vulnérables et sujets à des actions malveillantes pouvant mener à des menaces sérieuses pour une société hyperconnectée.

Une diversification d'usages

Les objets connectés sont hétérogènes dans leur nature, leur usage et leur fonctionnement. Les phénomènes du « fait maison » (*maker kit*) et du "DIY" (*Do It Yourself*) se développent. Ils passent notamment par la transformation d'éléments divers en objets connectés par l'apposition de moyens de communication. Ainsi, les appareils ne sont pas toujours reconnaissables. Certains dispositifs demeurent cachés dans leur environnement et émettent une faible signature. Nous pouvons citer l'exemple d'une caméra embarquée dans un ours en peluche ou celui d'un déodorant contenant un système de stockage Wi-Fi avec des données à caractère pornographique mettant en scène des mineurs. Ces situations rencontrées proviennent de perquisitions domiciliaires.

Un autre phénomène réside dans le détournement de l'usage initial, notamment pour cacher des agissements. Le cas du réseau de communication sans infrastructure, développé lors des manifestations à Hong Kong en 2014 (Dunand, 2014), en est une illustration. Cette structuration de l'espace numérique s'appuie sur une application exploitant un réseau Bluetooth. L'usage des technologies de communication, détournées de leur fonction primaire, se meut en nouvelles solutions ou services.

La proximité entre l'objet et l'humain pose des interrogations sur le potentiel destructeur du premier dans le cadre d'un piratage d'une infrastructure connectée par un individu ou par un groupe aux intentions hostiles ou malveillantes. À ce phénomène, les objets ouvrent de nouvelles surfaces d'attaque pour intercepter des informations dans une logique de « guerre électronique ». L'utilisation de données personnelles ou de fonctionnement transitant sur les réseaux sans l'autorisation des propriétaires est la norme et complexifie la donne. Néanmoins, le risque est maîtrisable par une connaissance fine des systèmes et de leur fonctionnement.

Conclusion

L'importance des objets connectés dans le cadre des missions judiciaires n'est plus à démontrer. En tant que témoins de nos activités quotidiennes, ils sont des sources riches d'informations dans la recherche de la vérité et la résolution des enquêtes. Ces traces numériques soulèvent cependant de nombreuses questions, notamment dans l'appréhension de l'écosystème avec pertinence : son identification, la collecte et l'analyse de l'information au regard d'un contexte. Cette démarche passe par la sensibilisation, l'acculturation et la formation des acteurs cyber, notamment par l'apprentissage d'actes réflexes ainsi que par la production de solutions techniques pour le primo-intervenant et le technicien du numérique. Face à la dispersion de la donnée entre cyberespace-espace physique et la pluralité des écosystèmes, la démarche d'investigation est nécessairement coordonnée et structurée.

Les objets connectés sont également des facteurs externes à prendre en considération dans un raisonnement tactique pour le succès d'une intervention et d'une mission. En effet, une manœuvre et son effet majeur peuvent être compromis par ce type de dispositifs et l'externalisation de la donnée. Ces équipements constituent une contrainte dans la recherche d'une discrétion ou d'un élément de surprise lors d'une progression. Détournés de leurs usages premiers, les objets connectés sont susceptibles d'attenter à la vie des unités d'intervention. Il est donc primordial pour les acteurs d'identifier en amont les dispositifs, afin d'adapter une réponse opérationnelle satisfaisante à la menace.

Bibliographie

BOUCHAUD F. (2021), *Analyse forensique des écosystèmes intelligents communicants de l'Internet des objets*, thèse de doctorat, Université de Lille.

CASSIDY M. (2018), "Fitbit offers key clue to slain San Jose woman's alleged 90-year-old killer", https://www.sfchronicle.com/crime/article/Fitbit-offers-key-clue-to-slain-San-Jose-13266777.php

CHAVEZ N. (2017), "Arkansas judge drops murder charge in Amazon echo case", https://edition.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html

COSQUER C. & LANCKRIET J. (2016), « Les objets connectés et la défense », *Revue défense nationale*, N° 787, pp. 97-103.

DUNAND C. A. (2014), « À Hong Kong, les manifestants adoptent FireChat pour communiquer sans réseau », https://www.lesechos.fr/30/09/2014/lesechos.fr/0203817723785_a-hong-kong--les-manifestants-adoptent-firechat-pour-communiquer-sans-reseau.htm

GASSER U., GERTNER N., GOLDSMITH J. L., LANDAU S., NYE J. S., O'BRIEN D., OLSEN M. G., RENAN D., SANCHEZ J., SCHNEIDER B. *et al.* (2016), *Don't panic: Making progress on the "going dark" debate*, Berkman Center Research Publication.

HAZANE E. (2018), « Sécurité numérique des objets connectes, l'heure des choix », https://www.frstrategie.org/sites/default/files/documents/publications/notes/2018/201815.pdf

LE MONDE (2016), « Le directeur du renseignement américain reconnaît s'intéresser aux objets connectés », https://www.lemonde.fr/pixels/article/2016/02/10/le-directeur-du-renseignement-americain-reconnait-s-interesser-aux-objets-connectes_4862587_4408996.html

THOMAS J. (2019), "How police unmasked 'Iceman' assassin behind one of Britain's most notorious gangland murders", https://www.liverpoolecho.co.uk/news/liverpool-news/how-police-unmasked-iceman-assassin-15649613

UNIT 42 (2020), "IoT Threat Report", https://unit42.paloaltonetworks.com/iot-threat-report-2020/

WILIAMS-GRUT O. (2018), "Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank", https://www.businessinsider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4?IR=T