RFC 9153 : Requirements and Terminology for the Drone Remote Identification Protocol (DRIP)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 février 2022

Date de publication du RFC : Février 2022

https://www.bortzmeyer.org/9153.html

Il y a aujourd'hui beaucoup plus de drones que d'avions pilotés. Ces drones, qui se déplacent dans un espace partagé, soulèvent un certain nombre de questions de sécurité, ce qui justifie des mécanismes obligatoires d'immatriculation et d'identification. Dans tous les pays, des règles imposent aux drones ou au moins à certains d'entre eux de diffuser leur identité. Mais, ensuite, une fois que l'observateur du drone a cette identité, qu'en fait-on ? Le but du projet DRIP <https://datatracker.ietf.org/wg/drip/> à l'IETF est de mettre au point des mécanismes pour utiliser cette identité. Ce RFC est le premier du projet, dédié à établir les exigences pour les futurs protocoles. Ce n'est pas gagné, vu qu'il y a beaucoup de grosses organisations sur le chemin qui vont privilégier des solutions fermées.

Pour aider à comprendre le problème, imaginons le scénario suivant. Un gardien fait sa ronde autour d'une centrale nucléaire. Un drone approche. Sa présence ici est-elle normale ? Est-il encore sous contrôle ou bien a-t-il échappé à son propriétaire ? Peut-on contacter son propriétaire pour vérifier ? S'il s'agissait d'un avion piloté traditionnel, les règles de circulation aérienne imposeraient tout un tas de contraintes au pilote (par exemple d'enregistrement de son vol à l'avance), qui permettraient d'éviter des incertitudes. On ne peut pas imposer des procédures aussi lourdes à un simple drone de loisirs. Mais on ne peut pas laisser non plus l'espace partagé qu'est l'air sans règles minimales. Prenons un autre scénario : un drone se promène au-dessus de votre jardin. Il a sans doute une caméra, comme la plupart des drones. Comment faire en sorte qu'il déguerpisse au lieu de vous filmer tranquillement en train de bronzer ? Peut-on lui tirer dessus, comme ça se fait aux États-Unis (« "*get off my lawn*" »), s'il ne répond pas ? Faut-il faire des sommations, et comment ? Comme l'analyse correctement la Quadrature du Net, le danger des drones ne vient pas que d'individus malveillants, une utilisation de ces engins par l'État crée également de nombreux risques <https://www.laquadrature.net/loidrone/>.

Depuis quelques années, de nombreuses règles ont été édictées dans divers pays. Ainsi, en France, l'arrêté du 29 décembre 2019 <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000039685188> impose la signalisation électronique des appareils pour tous les drones de plus de 800 grammes (cet article du Monde résume les obligations <https://www.lemonde.fr/

pixels/article/2020/07/06/drones-la-signalisation-electronique-des-appareils-devient-o
6045377_4408996.html>). Le drone doit être enregistré sur le site officiel AlphaTango <https:
//alphatango.aviation-civile.gouv.fr> (uniquement le drone, pas chaque vol, contrairement aux obligations des avions). Aux États-Unis, il existe des règles similaires <https://www.federalregister.
gov/documents/2021/01/15/2020-28948/remote-identification-of-unmanned-aircraft>.
La plupart du temps, l'obligation minimale est que le drone diffuse son identité, de la même façon qu'une voiture a une plaque d'immatriculation. Mais cette règle est très insuffisante pour répondre à tous les scénarios. Le drone peut facilement mentir sur son identité. Et puis à quoi sert cette identité si elle ne fournit pas de moyen de retrouver le propriétaire ? Et ne serait-ce pas souhaitable d'avoir un moyen de contacter celui-ci en temps réel ? Ces questions ne sont pas évidentes et, comme toutes les questions liées à la sécurité, soulèvent d'innombrables problèmes politiques, juridiques et techniques. L'IETF se concentre sur une partie limitée de ces problèmes : ne pouvons-nous pas utiliser notre expérience en matière de protocoles réseau pour développer des mécanismes permettant de retrouver des données sur le drone à partir de son identité et, pourquoi pas, permettant de communiquer avec lui ? Voyons d'abord en détail le problème, les exigences de notre RFC pour les futurs protocoles ne seront présentées qu'à la fin de cet article.

Ah, si vous voyez ce drone, c'est le mien :

La section 1 de notre RFC détaille pourquoi les drones posent des problèmes. Il existe plusieurs types de drones (à aile fixe, à aile tournante, capables de décollage vertical ou non, avec un ou plusieurs moteurs…). Le type le plus répandu et le plus connu, notamment grâce aux petits drones de loisir, est le multi-moteur à ailes tournantes (multicoptère). Disposant de systèmes de stabilisation automatiques, ils peuvent être pilotés par des amateurs, contrairement aux avions et hélicoptères. Mais il existe aussi des drones dont la taille et le prix rappelle davantage un avion. Être pilotés à distance par un humain tenant un "*joystick*" n'est pas la seule possibilité : doté d'un récepteur GPS, certains drones sont partiellement autonomes et, dans le futur, seront totalement autonomes.

Un petit drone, comme celui que vous achetez pour quelques dizaines d'euros en magasin, a des propriétés importantes pour la sécurité de l'espace aérien :

— ils sont nombreux,
— il est difficilement détectable par les radars,
— s'il est bruyant, voire insupportable, à courte distance, il est en général indétectable au bout de quelques centaines de mètres, alors qu'il peut couvrir cette distance rapidement ; un drone grand public peut faire 500 mètres en 13 secondes,
— il vole à très basse altitude,
— il est souvent piloté par un amateur sans vraie formation,
— très manœuvrant, il peut passer sous les arbres, rentrer dans un immeuble, etc.

Un drone peut donc être très utile pour l'espionnage, voire l'attaque. Il peut porter une caméra pour surveiller, et des explosifs pour attaquer (cf. l'attentat contre le premier ministre irakien <https://www.
liberation.fr/international/moyen-orient/irak-le-spectre-des-milices-derriere-lattenta
HFFY52XAVNGTXLP6SRSPG6B3CA/> en novembre 2021). Même sans explosifs, le drone peut jouer un rôle de projectile, involontaire ou volontaire. Un article de Kaspersky <https://www.kaspersky.
fr/blog/drone-incidents/12439/> donne une bonne idée des dangers possibles (mais notez qu'il est publié par une entreprise qui vend des solutions <https://www.kaspersky.fr/blog/
antidrone-under-the-hood/12434/> et peut donc être soupçonnée de dramatiser).

Il n'y a évidemment pas de solution magique à ces risques mais la plupart des approches nécessitent a priori qu'on découvre un **identificateur** du drone, qu'on ait une solution RID ("*Remote IDentification and tracking*"). Dans le scénario typique de RID, un ou plusieurs drones volent dans un espace restreint, et des observateurs, certains ayant un rôle particulier (policiers, par exemple) et d'autres étant du grand public, veulent obtenir un identificateur, qui va être le point de départ de leurs actions (s'informer sur

ce drone, peut-être le contacter). Il est donc prévu un ou plusieurs **registres** d'identificateurs, et des informations associées. Il existe déjà des normes pour cela, comme la F3411-19 <https://www.astm.org/f3411-19.html>, développée par le comité F38 de l'ASTM. Elle coûte 91 dollars étatsuniens. Comme beaucoup de normes développées par des organismes privés, elle n'est pas librement et gratuitement disponible, mais on peut apparemment trouver des brouillons en ligne <https://github.com/opendroneid/specs>. F3411-19 est la référence dans ce domaine, normalisant les messages que le drone doit envoyer pour annoncer son identifiateur mais, pour l'instant, c'est à peu près tout, on ne peut pas forcément faire grand'chose de cet identificateur. Elle ne précise pas comment l'observateur se renseigne sur les personnes ou organisations derrière un identificateur. Elle ne traite pas la communication entre drones ou avec l'observateur. Elle n'a pas de mécanisme d'authentification de l'identificateur. Le RFC, étant surtout développé par des États-suniens, est très inspiré par le travail de l'ASTM, qui ne s'applique pas forcément partout dans le monde. En Europe, ASD-STAN, associée à CEN, publie une norme DIN EN 4709-002 :2021-02 <https://asd-stan.org/downloads/din-en-4709-0022021-02/> (également chère et pas libre). Un résumé est disponible en ligne <https://asd-stan.org/wp-content/uploads/ASD-STAN_DRI_Introduction_to_the_European_digital_RID_UAS_Standard.pdf>. Cette norme décrit un système de DRI ("*Drone Remote Identification*") où le drone diffuse par radio :

— le numéro d'identification de l'opérateur du drone (qui doit donc s'enregistrer),
— celui du drone (en suivant CTA2063A <https://shop.cta.tech/products/small-unmanned-aerial-sys - aussi désignée ANSI/CTA/2063-A, enfin une norme gratuitement disponible mais attention, il faut laisser plein de données personnelles pour l'obtenir).
— l'heure qu'il est, la position du drone (en trois dimensions),
— la vitesse et le cap du drone,
— la position du pilote ou, à défaut, la position d'où le drone a décollé.

Un exemple d'identificateur de drone (celui donné par la norme) est `MFR1C123456789ABC`. (Le C en cinquième position est l'encodage de la longueur du numéro de série, ici `123456789ABC`).

Même avec ces normes, de nombreux problème subsistent. Si trois drones sont proches, chacun diffusant son identité, et qu'un seul des trois a un comportement inquiétant, comment distinguer les trois identités ? Et puis les informations envoyées peuvent être erronnées (les drones bon marché n'incluent pas du matériel de mesure perfectionné) voire mensongères, notamment si le drone est malveillant.

Notez aussi que les groupes techniques comme DRIP <https://datatracker.ietf.org/wg/drip/> ne peuvent qu'établir des normes techniques. Définir des règles politiques est une autre affaire. Et les faire respecter sera largement l'affaire des CAA.

Autre problème, comme le drone diffuse des informations en clair, tout le monde peut les capter et certaines informations (comme l'identificateur de l'opérateur) sont des données personnelles, ce qui soulève des questions de vie privée. On a là un beau débat politique en perspective, entre intimité et transparence.

Le RFC note qu'un déploiement massif d'un système de RID ("*Remote IDentification and Tracking*") est à la fois urgent et important. Le déploiement doit être massif car, comme le dit le RFC, « quel serait l'intérêt des plaques minéralogiques si seulement 90 % des voitures en avaient ? ».

Un autre défi des systèmes d'identification réside dans le caractère capricieux des ondes radio. Elles peuvent être bloquées par des bâtiments ou du feuillage. Si le drone émet avec davantage de puissance, il va épuiser rapidement sa batterie. Et il aggravera la congestion dans cet espace partagé (d'autant plus que le drone émet dans des fréquences où une licence n'est pas nécessaire). Bref, d'une manière générale, la liaison radio sera lente et non fiable.

En parlant de batterie, il faut noter que le drone est typiquement un objet contraint (au sens du RFC 8352 [1]). Son « budget » en énergie, puissance de calcul et poids (ce qu'on désigne en général par le sigle CSWaP, "*Cost, Size, Weight, and Power*", parfois écrit $SWaP) est très limité. Cela impose des protocoles de communication simples et frugaux, ce qui va rendre difficile l'utilisation de la cryptographie. Actuellement, il y a zéro authentification : un drone mensonger peut annoncer l'identificateur qu'il veut, sans qu'on puisse vérifier. (Dans des réunions, j'ai entendu des affirmations ridicules, comme de confondre la somme de contrôle avec un mécanisme d'authentification. Comme souvent en cybersécurité, on entend beaucoup de n'importe quoi dans les réunions.)

Et il n'y a pas que le drone, il y a aussi la machine de l'observateur. Dans des zones reculées, on ne peut pas compter sur une connectivité Internet permanente, et c'est une des raisons du choix du "*Broadcast RID*" (le drone diffuse son identificateur, également appelé "*Direct ID*") plutôt que du "*Network ID*" (l'observateur obtient l'identificateur via un réseau public, typiquement l'Internet). Mais si vous voulez en savoir plus sur ce débat "*Network ID*" vs. "*Broadcast ID*", voyez l'article « "*Why Did the FAA Go with Broadcast Remote ID for Drones Over Network?*" <https://www.commercialuavnews.com/regulations/why-did-the-faa-go-with-broadcast-remote-id-for-drones-over-network> ».

Bref, les mécanismes actuellement normalisés et déployés sont très insuffisants. Le projet DRIP de l'IETF <https://datatracker.ietf.org/wg/drip/> vise, non pas à remplacer les normes existantes, mais à les compléter pour traiter les manques. Ce RFC est le cahier des charges du projet.

Le monde des drones utilise une grande quantité d'acronymes. La section 2 du RFC en donne une liste complète, mais il faut au moins connaitre :

— CAA ("*Civil Aviation Authority*"), l'autorité de régulation de l'aviation comme la DGAC en France ou la FAA aux États-Unis. Le milieu aérien, partagé et complexe, est très régulé dans tous les pays.
— DRI ("*Direct Remote Identification*"), la possibilité d'obtenir l'identificateur d'un drone (le cœur du système).
— LOS ("*Line Of Sight*"), la ligne qui va mener au drone pour le contrôler. Ce n'est pas forcément un lien visuel (voir « VLOS »), le pilote peut obtenir l'information sur le drone par d'autres moyens. Lorsque le drone n'est pas sur la LOS, il est incontrôlable (sauf s'il peut agir de manière autonome).
— RID "*Remote IDentification*" ou UAS RID, le système qui permet aux observateurs d'obtenir l'identificateur du drone et, par extension, l'identificateur du drone.
— UA ("*Unmanned Aircraft*"), un drone.
— UAS ("*Unmanned Aircraft System*"), le drone, et tout ce qui lui permet de voler et d'être piloté (la télécommande, par exemple).
— UAS ID ("*Unmanned Aircraft System IDentifier*"), l'identificateur de l'UAS (en fait, en pratique, c'est plutôt celui de l'UA).
— VLOS ("*Visual Line Of Sight*"), lorsque le pilote voit son drone. Dans certains pays, la reglémentation peut imposer que le vol du drone se fasse en permanence à vue, et que le pilote ait donc une VLOS avec son engin, ce qui interdit par exemple de le faire voler derrière un bâtiment.

Pour les RID, les identificateurs des drones, il existe plusieurs textes normatifs. Le plus répandu est F3411-19, déjà mentionné, qui décrit les notions de "*Network RID*" et "*Broadcast RID*". Pour le premier, l'observateur va récolter l'information via le réseau (le drone s'étant au préalable enregistré, on est dans le "*publish-subscribe*"), alors que dans le cas du second, il va écouter directement ce que diffuse le drone par ondes radio. Comme l'observateur, le pilote du drone et surtout le drone lui-même n'ont pas forcément d'accès à l'Internet, c'est le "*Broadcast RID*" qui est privilégié. Il fonctionne donc indépendamment de l'Internet.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8352.txt

Le "*Broadcast RID*" soulève de nombreux problèmes techniques, notamment en raison des caractéristiques physiques des ondes radio. Si on utilise Bluetooth, on a de sérieuses contraintes de taille des données, au cas où on veuille transmettre, en sus de l'identificateur, des informations de position, de vitesse et de route. En outre, les normes existantes ne standardisent pas les couches basses (Bluetooth 4, 5, Wifi NAN, Wifi Beacon...), donc il sera difficile de capter tous les drones, et surtout pas avec n'importe quel ordiphone <https://github.com/opendroneid/receiver-android/blob/master/supported-smartphones.md>, le drone émettant peut-être avec une technologie que l'ordiphone ne connait pas. En outre, sur beaucoup d'ordiphones, on n'a pas accès direct à Bluetooth (cf. les problèmes de l'application TousAntiCovid) et/ou pas accès aux paquets bruts, ce qui va compliquer la vie des développeurs. (Le projet AltBeacon <https://altbeacon.org/> vise à traiter ce problème.)

Comment est attribué le RID ? F3411-19 propose plusieurs méthodes :

— Un identificateur statique attribué par le fabricant du drone, comme prévu par la norme ANSI/CTA-2063-A <https://shop.cta.tech/products/small-unmanned-aerial-systems-serial-numbers>,
— Un identificateur statique attribué par une CAA, comme cela se fait aujourd'hui pour les avions,
— Un UUID (RFC 9562), statique ou dynamique, attribué par un système spécifique aux drones (une nouvelle autorité ?),
— Un identificateur dynamique spécifique au vol.

Actuellement, l'Union Européenne impose <https://eur-lex.europa.eu/eli/reg_del/2019/945/oj> le premier type, les États-Unis le premier ou le troisième. La situation est compliquée, et le choix fait a des implications évidentes en terme de vie privée (un identificateur statique permet de suivre à la trace un drone). C'est d'autant plus important que cette information, étant diffusée unilatéralement, ne peut pas être chiffrée, les protocoles de type défi-réponse étant inutilisables. Pour prendre un exemple, Amazon ne serait sans doute pas ravi qu'un concurrent puisse suivre précisement leurs drones de livraison.

La simple diffusion du RID est donc déjà un problème compliqué. Mais d'autres organismes que l'IETF s'en occupent. Par contre, cette diffusion laisse entier un autre problème : une fois qu'on a récupéré le RID, qu'en fait-on ? Comment, par exemple, communiquer avec le pilote du drone ? Si le message contenait, en sus de l'identificateur, la position du pilote, on peut toujours s'y rendre. Cela peut être lent, voire infaisable si le pilote est, par exemple, de l'autre côté d'une voie ferrée. Dans l'hypothèse où il existe un registre des identificateurs, associé à des informations de contact (comme on fait pour les noms de domaine), on pourrait imaginer que l'observateur regarde dans le registre (avec des protocoles comme RDAP ou whois) et appelle au téléphone le pilote. Reste à savoir si c'est une bonne idée que le pilote réponde alors que son attention devrait être concentrée sur le pilotage...

L'IETF, via son groupe DRIP, va donc tenter de développer des solutions pour :

— authentifier l'identificateur de drone,
— permettre l'interrogation d'un registre de ces identificateurs,
— faciliter la coordination entre observateurs pour qu'ils puissent vérifier collectivement ce que fait un drone,
— contacter le pilote.

Le but est évidemment que ces solutions reposent sur des normes ouvertes et accessibles. (Un certain nombre d'organisations font déjà du "*lobbying*" pour pousser au déploiement et à l'obligation légale de solutions privées et fermées, leur assurant le contrôle, et les revenus associés.)

Les normes existantes comme F3411-19 <https://www.astm.org/f3411-19.html> ne permettent pas cela, d'où ce cahier des charges du projet DRIP, dont les exigences forment la section 4 de notre RFC. Chacune est identifiée par trois lettres indiquant sa catégorie, puis un numéro. Ainsi, la première exigence est dans la catégorie des généralités et se nomme GEN-1 : « DRIP doit permettre d'authentifier les affirmations du drone » (puisque, actuellement, un drone peut raconter ce qu'il veut). Je ne vais pas vous lister toutes les exigences, seulement de quoi vous donner une idée du projet. Ainsi, GEN-2 suit GEN-1 en demandant qu'en outre, tous les messages du drone puissent être reliés à ceux qui prouvent

l'identité du drone (et pas uniquement parce que les messages sont émis depuis la même adresse MAC). GEN-3 impose qu'il existe un moyen de vérifier l'enregistrement du drone dans un registre, même en l'absence de connexion Internet (par exemple le drone pourrait diffuser un certificat signé par le registre). GEN-6 concerne la prise de contact, il faut qu'il existe un moyen de contacter le pilote. (Attention, comme tout ce cahier des charges, il s'agit d'une exigence technique, pas politique. L'IETF n'a pas l'autorité pour édicter des règles disant, par exemple, que le pilote doit accepter les communications entrantes. Elle dit juste qu'un moyen technique doit exister, mais son utlisation pourra, par exemple, être restreinte à des appelants identifiés et autorisés.) Un protocole envisagé pour cette communication est HIP <https://www.bortzmeyer.org/hip-resume.html>.

GEN-8 demande que tout cela fonctionne même si le drone (évidemment), son pilote et l'observateur sont en déplacement, GEN-9 veut un mode "*multicast*", et GEN-10 un moyen de superviser le bon fonctionnement du système (notamment pour le "*Network RID*").

La catégorie suivante concerne plus spécifiquement les identificateurs. ID-1 met une taille maximale à 19 octets (c'est une limite de F3411-19, sauf erreur). ID-2 dit que sur ces 19 octets au maximum, il faut placer un identificateur du registre. ID-4 exige que l'identificateur soit unique (ce qui est du simple bon sens) et ID-5, reprenant GEN-1, demande que le drone ne puisse pas mentir sur son identificateur. ID-6 veut qu'on puisse empêcher de suivre un drone ou son propriétaire à la trace (et il faut donc permettre des identificateurs qui ne soient pas statiques sur le long teme). Là encore, rappelez-vous l'avertissement de la catégorie précédente : DRIP ne définit pas une politique, l'activation ou non de la technique demandée par ID-6 n'est pas une question purement technique.

En parlant de gêner la surveillance, la troisième catégorie concerne la vie privée (voir aussi la section 7). PRIV-1 rappelle l'importance de protéger les données privées (par exemple en ne distribuant pas le nom et l'adresse du pilote publiquement) et PRIV-4 demande pour cela que le système d'enregistrement sépare ce qui est public et ce qui ne l'est pas (données personnelles, par exemple).

Et les registres ? Sur l'Internet, il existe de nombreux types de registres, comme les registres de noms de domaine ou les RIR. Certains problèmes, comme l'arbitrage entre les exigences opérationnelles (où on voudrait obtenir facilement beaucoup d'informations sur les titulaires des noms de domaine) et celles de vie privée, sont bien connues depuis longtemps (le « problème whois » de l'ICANN, par exemple). J'ai pris plusieurs exemples tirés des registres de noms de domaines car c'est là où je travaille. La quatrième et dernière catégorie d'exigences DRIP concerne précisément les futurs registres de drones. En raison des limites de taille très strictes sur ce que le drone peut diffuser, il est essentiel de disposer de registres permettant l'accès à davantage d'informations. REG-1 commence par demander qu'il existe un moyen d'interroger le registre (la solution évidente étant RDAP, RFC 9082). Ce moyen doit (exigence REG-2), contrairement à whois (RFC 3912), permettre l'accès différencié (davantage d'informations pour certains clients). REG-3 réclame qu'on puisse ajouter, retirer et modifier de l'information dans le registre (là, la solution évidente est EPP, RFC 5730). Notez qu'une présentation sur l'utilisation de registres avait été faite lors d'une réunion professionnelle des acteurs du monde des registres : les supports <http://regiops.net/wp-content/uploads/2020/06/Stuart-Card-Robert-Moskowitz-ROW9-presentation.pdf>.

Enfin, la section 6 du RFC concerne l'analyse de sécurité du futur système. Quelles que soient les solutions adoptées, il faudra faire attention aux attaques Sybil, aux attaques par déni de service utilisant, par exemple, de nombreux messages incorrectement signés, aux attaques de l'Homme du Milieu, etc. On pourra voir aussi des attaques plus subtiles comme, suggère le RFC, un drone de petite taille, a priori pas très effrayant, et qui s'authentifiera proprement, mais derrière lequel surgira le vrai attaquant.

Pour les curieuses et les curieux, je recommande également l'annexe A du RFC, qui discute les choix effectués dans ce RFC et leurs raisons. Par exemple, l'analogie avec les plaques d'immatriculation des

voitures, souvent utilisée dans les débats sur l'identification des drones a ses limites. Dans certains pays, par exemple des États des USA, n'importe qui peut accéder, parfois même gratuitement, aux données du registre, et donc aux informations personnelles sur les propriétaires de véhicules. Faut-il faire pareil pour les drones ? Même en Europe, si le registre n'est pas accessible, en revanche, les voitures ont un identificateur statique stable, qui peut faciliter certaines formes de surveillance. Veut-on cela pour les drones ?

Les avions (civils) pilotés et les bateaux ont l'habitude depuis longtemps de diffuser leur identité à qui veut écouter (le transpondeur pour les avions). D'excellentes et utiles applications comme OpenSky et Flightradar24 exploitent cette information. Souhaite-t-on un même fonctionnement pour les drones ? Outre les questions politiques, cela peut poser des problèmes techniques, par exemple parce que le nombre de codes utilisables est limité et qu'il y a beaucoup plus de drones que d'avions. Avec les 24 bits typiquement utilisés, on ne pourrait traiter que seize millions de drones, ce qui est loin des nombres envisagés.

Les drones qui diffusent leur identité le font en Wi-Fi ou en Bluetooth. Ces techniques ont l'avantage d'être très répandues, aussi bien du côté des drones que des observateurs (tous ont un ordiphone), peu chères, libres d'usage, et elles permettent la diffusion. Par contre, leur portée est faible. Il pourrait être intéressant de travailler sur des technologies conçues pour les grandes distances (comme WiMAX), ou pour les réseaux de capteurs (comme LoRA).

Voilà, le groupe DRIP est évidemment au travail pour mettre au point des protocoles correspondant à ces exigences. Le problème posé par les drones ne peut que devenir de plus en plus sérieux, notamment parce que leur discrétion augmentera. Dans les romans de la série Harry Potter (par J. K. Rowling), une journaliste-sorcière sans scrupule peut se transformer en insecte pour aller espionner les gens chez eux. Un drone suffisamment petit pour être quasiment indétectable serait un cauchemar pour la vie privée…

Pour en savoir plus, quelques ressources utiles :

— Pour développer des solutions ouvertes, le projet OpenDroneID <https://www.opendroneid.org/>.
— Autre projet analogue, Paparazzi UAV <https://wiki.paparazziuav.org/>.
— La vidéo de l'atelier drones de CEN et CENELEC du 9 février 2021. <https://www.youtube.com/watch?v=bf5JtEd7TVg>. Les organisateurs sont deux organisations de normalisation traditionnelles.
— Un résumé de la situation européenne, par ASD-STAN <https://asd-stan.org/wp-content/uploads/ASD-STAN_DRI_Introduction_to_the_European_digital_RID_UAS_Standard.pdf> (une organisation de normalisation spécialisée dans l'aéronautique).
— Un intéressant projet d'étudiants de l'université de Link[Caractère Unicode non montré [2]]ping sur DRIP <https://www.ida.liu.se/~TDDE21/info/TDDE21_DRIP_finalreport_2020.pdf> et sur l'utilisation de HIP pour contacter le drone <https://www.ida.liu.se/~TDDE21/info/TDDE21_HIPv2_finalreport_2020.pdf>.
— La chaire de recherche sur les drones <http://drone-chair.enac.fr/> à l'ENAC. Et la volière de l'ENAC <https://www.enac.fr/fr/voliere-drones-toulouse-occitanie> (une volière étant un endroit fermé où on peut faire des expérimentations avec les drones).
— Et enfin, divers dispositifs de réalité augmentée <https://lii.enac.fr/portfolio/supporting-drones-c> pour aider à piloter les drones.

2. Car trop difficile à faire afficher par LaTeX