



LIGNES DIRECTRICES SUR LES RISQUES ET LES MESURES D'ATTÉNUATION LIÉS À L'UTILISATION DE DRONES

CENTRE DE LA SÉCURITÉ DE LA RECHERCHE

Les systèmes d'aéronefs sans pilote, communément appelés drones, sont devenus des outils de plus en plus courants dans la recherche académique et appliquée. Leur capacité à transporter des capteurs, à recueillir des données à haute résolution et à accéder à des zones qui peuvent être éloignées, dangereuses ou difficiles d'accès a conduit à leur adoption dans un large éventail de disciplines, notamment les sciences de l'environnement, l'écologie, l'archéologie, l'ingénierie, l'agriculture, la santé publique, les géosciences et les sciences sociales.

Parallèlement, le marché mondial des drones et des technologies compatibles avec les drones s'est rapidement développé. Les chercheuses et chercheurs ont maintenant accès à un nombre croissant de plateformes commerciales, de fabricants et de fournisseurs de services opérant dans plusieurs juridictions. Bien que cela offre de nouvelles possibilités, cela introduit également de nouveaux risques pour la sécurité de la recherche liés à la cybersécurité, à la vie privée, à la protection des données et à la souveraineté des données.

Les données saisies par les drones peuvent révéler des informations sensibles sur les zones dans lesquelles les drones opèrent ainsi que sur les méthodes d'utilisation des drones. Si les drones ne sont pas achetés auprès de fabricants canadiens ou de fabricants dans des pays qui entretiennent une relation commerciale de confiance avec le Canada, leurs composants connectés et leurs périphériques associés peuvent transférer ces renseignements à d'autres juridictions, à l'insu ou non de l'utilisateur. Des efforts devraient également être déployés pour s'assurer que les drones achetés auprès de sources canadiennes et fiables ne sont pas des drones « en marque blanche » ou ne contiennent pas de composants provenant d'autres juridictions. Par conséquent, l'acquisition et l'utilisation de drones dans la recherche nécessite une diligence raisonnable additionnelle et la mise en œuvre de mesures d'atténuation appropriées pour faire face à ces risques.

Les chercheurs et les établissements de recherche sont fortement encouragés à tenir compte de ces lignes directrices lorsqu'ils cernent et atténuent les risques associés à la recherche impliquant des drones, y compris lorsqu'ils remplissent les [formulaires d'évaluation des risques](#) dans le cadre des demandes de subvention assujetties aux [Lignes directrices sur la sécurité nationale pour les partenariats de recherche](#).

RISQUES

Conformément aux directives établies par le Centre canadien pour la cybersécurité (CCC), voici deux facteurs de risque importants à prendre en compte lorsque vous travaillez avec des drones :

SÉCURITÉ DES DONNÉES

Les drones sont des appareils non fiables et peuvent présenter un risque important pour votre organisation lorsqu'ils sont directement ou indirectement connectés à votre réseau. Leur connexion peut être exploitée par les acteurs malveillants comme vecteur d'attaque ou utilisée pour obtenir un accès à distance à votre environnement.

Certains drones nécessitent également l'utilisation de services infonuagiques pour accéder aux métadonnées de vol chiffrées stockées sur le drone lui-même. Si ces services infonuagiques sont basés à l'extérieur du Canada ou d'un pays partageant les mêmes valeurs, il est fort possible que les données recueillies lors du vol puissent être utilisées par des acteurs malveillants.

BROUILLAGE PAR SATELLITE

Les drones peuvent être induits en erreur par l'interférence de la navigation par satellite en brouillant ou en falsifiant les signaux pour créer de faux signaux et empêcher la communication avec le drone. Cela peut entraîner une perte totale de contrôle du drone par l'utilisateur et peut avoir un impact négatif sur les résultats de recherche prévus, ainsi que de créer un danger si les drones sont utilisés dans des zones densément peuplées.

Avant le déploiement du drone pour leur projet, il est recommandé aux chercheuses et chercheurs de travailler avec l'équipe de sécurité informatique de leur établissement et leur bureau de la sécurité de la recherche (le cas échéant) pour effectuer une évaluation des risques liés au fabricant du drone et de tout danger physique et de cybersécurité potentiel afin d'être bien placés pour atténuer ces risques.

MESURES D'ATTÉNUATION

Dans la mesure du possible, le Centre de la sécurité de la recherche recommande d'éviter les drones et leurs composants provenant de pays qui n'entretiennent pas de relations commerciales de confiance avec le Canada.

La meilleure mesure d'atténuation de ces risques consiste à s'approvisionner en drones et en périphériques connexes auprès d'entreprises qui les fabriquent au Canada ou auprès de pays partenaires commerciaux dignes de confiance. Les fournisseurs de confiance devraient intégrer des normes de cybersécurité sécurisées dès la conception et par défaut et devraient donner la priorité à la sécurité de leurs clients en tant qu'exigence opérationnelle fondamentale.

Les fournisseurs de confiance devraient également vendre des drones qui ne sont pas des versions « en marque blanche » de drones provenant de sources non fiables et qui n'intègrent pas de composants provenant de sources non fiables.

Les drones fabriqués dans des pays qui sont des partenaires commerciaux de confiance du Canada et qui n'intègrent pas de telles normes et pratiques présentent des risques de sécurité des données similaires à ceux des drones fabriqués dans des pays qui n'ont pas de relations commerciales de confiance avec le Canada.

Dans des circonstances exceptionnelles où les drones ne peuvent pas être achetés auprès d'un fournisseur de confiance, des mesures d'atténuation supplémentaires sont fortement recommandées pour traiter de manière appropriée les risques associés à la sécurité de la recherche et à la cybersécurité. Il s'agit notamment des éléments suivants :

LE DRONE DOIT ÊTRE CONTRÔLÉ À L'AIDE D'UN CONTRÔLEUR DÉDIÉ OU AUTONOME.

Le contrôleur ne doit pas être connecté à aucun autre dispositif ou réseau, à l'exception du drone lui-même.

LE DRONE DOIT ÊTRE UTILISÉ UNIQUEMENT EN MODE HORS LIGNE.

La plupart des fabricants de drones permettent aux particuliers d'utiliser le drone et ses logiciels connexes en mode hors ligne uniquement. Pour faire cela efficacement, tous les paramètres du drone doivent être basculés en mode hors ligne et vous devez vous assurer que toutes les données recueillies par le drone sont stockées localement.

LE LOGICIEL DE GESTION DES DONNÉES DU DRONE DOIT ÊTRE UTILISÉ EXCLUSIVEMENT EN MODE HORS LIGNE.

Cela peut être fait efficacement en installant le logiciel du fabricant du drone sur un appareil qui ne peut pas être connecté à l'Internet (par exemple, un ordinateur portable dont les puces WiFi et Bluetooth ont été retirées).

- De nombreux fabricants de drones ont besoin d'un service infonuagique pour déchiffrer leurs données afin d'accéder aux métadonnées des carnets de vol. Si les serveurs de ce service infonuagique ne sont pas situés au Canada ou dans des pays partageant les mêmes valeurs, ces renseignements peuvent être accessibles aux services de sécurité et de renseignement étrangers au détriment de la sécurité nationale canadienne. Par conséquent, ces services ne devraient pas être utilisés.
- Si l'accès à la télémétrie de vol ou aux métadonnées du drone est nécessaire, le drone peut plutôt être modifié pour installer un module GPS tiers provenant d'un fournisseur de confiance qui peut fournir des informations telles que la vitesse de vol, la hauteur et la position, selon les besoins.

PLUS D'INFORMATION

Pour obtenir de plus amples renseignements sur les considérations de cybersécurité liées à l'utilisation de drones, nous vous encourageons à consulter des experts canadiens en cybersécurité. Vous pouvez également consulter les conseils utiles publiés par le CCC [ici](#).

Si vous avez des questions propres à un projet concernant les drones ou les mesures d'atténuation des drones, n'hésitez pas à communiquer avec le bureau de la sécurité de la recherche de votre établissement ou directement avec le [Centre de la sécurité de la recherche](#).