Les drones, véritables chevaux de Troie ukrainiens : une nouvelle frontière dans la cyberguerre

Le 10 avril 2025 par Miriam McNabb

Comment les drones équipés de logiciels malveillants façonnent les conflits modernes et ce que cela signifie pour la sécurité mondiale des drones

L'utilisation par l'Ukraine de drones équipés de logiciels malveillants pour saboter des systèmes russes capturés marque une nouvelle frontière dans la guerre cyberphysique – une tactique qui souligne les préoccupations mondiales plus larges concernant la sécurité des drones. Les forces ukrainiennes ont intégré des logiciels malveillants dans leurs drones afin de contrecarrer les tentatives russes de réutilisation ou de rétro-ingénierie de cette technologie. Cette innovation a non seulement un impact sur le champ de bataille, mais fait également écho aux débats actuels sur les risques liés à la chaîne d'approvisionnement des drones.

Comment fonctionnent les drones ukrainiens équipés de logiciels malveillants

L'Ukraine a développé une approche multicouche pour intégrer des logiciels malveillants à ses drones, créant ainsi un puissant outil de perturbation et de collecte de renseignements. Ces drones sont programmés avec un logiciel malveillant qui s'active dès leur capture et cible les forces russes de multiples façons. Le logiciel malveillant existe en trois variantes principales, chacune conçue pour atteindre des objectifs spécifiques :

- **Sabotage matériel** : les logiciels malveillants de base se déclenchent lors de la connexion aux systèmes ennemis, brûlant physiquement les ports USB ou endommageant les composants internes pour empêcher l'extraction ou la réutilisation des données.
- **Verrouillage du système** : les versions intermédiaires ciblent les puces embarquées, bloquant les mises à jour du micrologiciel et désactivant les composants critiques, rendant ainsi le drone inutilisable.
- **Cyber-espionnage secret** : les logiciels malveillants avancés restent indétectables jusqu'à ce qu'ils atteignent le territoire ennemi, où ils détournent les systèmes de contrôle pour rediriger les drones ou géolocaliser les opérateurs russes qui tentent de les réutiliser.

Cette stratégie à plusieurs niveaux assure une perturbation immédiate tout en offrant des avantages à long terme en matière de renseignement. Par exemple, des logiciels malveillants avancés peuvent exposer les emplacements des opérateurs russes ou détourner des drones reconvertis pour un usage ukrainien. En intégrant ces capacités, l'Ukraine limite la capacité de la Russie à rétroconcevoir sa technologie et retarde le développement de mesures anti-drones efficaces. Comme le rapporte *Forbes* , ces tactiques mettent en évidence l'imbrication croissante des cybercapacités et des outils de guerre physique.

Parallèles avec les préoccupations américaines

Bien qu'il n'existe aucun cas confirmé de logiciels malveillants étrangers dans des drones commerciaux, le conflit entre l'Ukraine et la Russie illustre des vulnérabilités théoriques qui correspondent aux débats de sécurité américains.

Les États-Unis ont restreint l'activité des entreprises chinoises de drones en raison de risques d'espionnage et ont récemment fait l'objet de sanctions de représailles de la part de la Chine, qui a inscrit 11 entreprises américaines de drones sur sa liste noire . Ces tensions illustrent comment les rivalités géopolitiques pourraient encourager l'insertion de codes malveillants, un scénario que les États-Unis cherchent à prévenir par des mesures telles que les règles proposées par le Département du Commerce pour la chaîne d'approvisionnement en drones.

La vue d'ensemble

La stratégie ukrainienne illustre la manière dont les capacités cybernétiques transforment la guerre, obligeant les adversaires à concilier innovation et sécurité. Pour l'industrie mondiale des drones, cela souligne la nécessité de diversifier les chaînes d'approvisionnement afin de réduire la dépendance aux rivaux géopolitiques, de renforcer les protocoles de cybersécurité pour les drones militaires et commerciaux, et d'investir dans l'industrie manufacturière nationale pour atténuer les risques de perturbation.