Combat de haute intensité, unités robotisées et cybersécurité

Thierry BERTHIER

Pilote du groupe « Sécurité - Intelligence Artificielle - Robotique » du Hub France IA
Directeur scientifique de la Fédération professionnelle européenne Drones4Sec
Chercheur associé CREC ESM Saint-Cyr

PLAN

I – Les métriques du combat de haute intensité

II – Focus sur la cybersécurité des drones aériens légers (UAV)

I – Les métriques du combat de haute intensité

1-1 - Activité et énergie de combat dans un volume durant une période temporelle

Nous considérons un cube de combat Hc (ou un hypercube x,y,z,c avec une dimension supplémentaire cyber) que nous projetons sur une surface afin de concentrer l'information utile. Nous définissons ensuite l'activité de combat présente dans le cube Hc durant une période temporelle Tc . La description des activités de combat doit tenir compte de l'ensemble des actions cinétiques, électromagnétiques, cybernétiques, psychologiques, informationnelles, opérant dans le cube Hc durant la période temporelle Tc.

Pour décrire l'activité de combat Ac , une méthode consiste à la vectoriser dans un espace à N dimensions où N est le nombre de caractéristiques de l'action de combat Ac = (a_1, a_2, …. , a_N). Les k premières coordonnées peuvent être réservées aux actions cinétiques. Les coordonnées suivantes décrivent l'activité électromagnétique dans le cube de combat. Les suivantes décrivent l'activité cybernétique dans le cube, puis l'activité informationnelle, renseignement et PsyOps.

La dimension N est par nature élevée car elle tient compte exhaustivement de l'ensemble des actions militaires.

1-1 - Activité et énergie de combat dans un volume durant une période temporelle

Une fois le vecteur d'activités Ac fixé, il faut lui adjoindre un vecteur de puissance Pc de même dimension dont les coordonnées p_i mesurent la puissance de chaque activité élémentaire du combat dans le cube Hc durant la période temporelle Tc.

Ainsi, Pc = (p_1 , p_2, …… , p_N) où p_i mesure la puissance (ou le poids) de l'action élémentaire a_i .

Dans un modèle linéaire, le produit scalaire :

$$Ec = < Ac , Pc > = \sum_{i=1}^{N} p_i \times a_i$$

est une mesure de « l'énergie » de combat, pondérée par la puissance, présente dans le cube Hc , durant la période temporelle Tc .

Dans un modèle non linéaire, l'énergie de combat déployée dans le cube Hc durant la période temporelle Tc s'écrit :

$$Ec = < \Phi(Ac) , Qc >$$

où Φ est un opérateur et Qc est un vecteur de poids adapté à Φ. L'introduction de non-linéarité permet de mesurer plus finement les interactions entre les différentes actions élémentaires de combat et leur puissances propres.

2 - Définition locale de l'intensité d'un combat sur un cube durant une période temporelle

L'intensité volumique de combat est définie sur le cube de combat Hc de volume V(Hc), et d'énergie Ec durant la période temporelle Tc par :

$$\mathrm{Ic} = \frac{Ec}{V(Hc) * Tc}$$

L'intensité surfacique de combat est définie sur la projection du cube de combat Hc (ou de l'hypercube intégrant la dimension cyber) de surface S(proj(Hc)), et d'énergie Ec durant la période temporelle Tc par :

$$\mathrm{Jc} = \frac{Ec}{S\big(proj(Hc)\big) * Tc}$$

Les intensités volumiques et surfaciques fournissent une métrique pour quantifier le combat de haute intensité.

3 - Intensité et énergie instantanée du combat

Le vecteur d'activité Ac et le vecteur puissance Pc dépendent de plusieurs variables dont la variable temporelle t.
L'énergie instantanée de combat s'exprime en fonction de t :

$$Ec(t) = < Ac(t) , Pc(t) > = \sum_{i=1}^{N} p_i(t) \times a_i(t) \quad \text{dans un modèle linéaire}$$

$$Ec(t) = < \Phi(Ac(t)) , Qc(t) > \quad \text{dans un modèle non linéaire}$$

L'intensité volumique instantanée de combat s'écrit $Ic(t) = \frac{Ec(t)}{V(Hc) * Tc}$

L'intensité du combat telle que nous la définissons s'applique à tous les types de conflits, passés ou à venir.

Nous pouvons par exemple l'évaluer sur deux exemples historiques de grandes batailles :

la bataille de Gergovie (52 avJC) et la bataille Napoléonienne de Borghetto (30 mai 1796).

Les derniers conflits (Syrie, Yémen, Arménie-Azerbaïdjan) nous montrent qu'il convient de catégoriser les intensités du combat en fonction des technologies employées.

4 - Energies du combat et intensités catégorielles

Nous avons défini l'énergie d'un combat pondéré par la puissance de l'armement mis en œuvre, dans un cube Hc , durant une période temporelle Tc par : Ec = < Ac , Pc > = $\sum_{i=1}^{N} p_i \times a_i$ ou plus généralement par Ec(t) = < Φ(Ac(t)) , Qc(t) >

Les termes de cette somme peuvent être ordonnés en sous-groupes correspondant aux familles de systèmes d'armes mis en œuvre. Nous réunissons toutes les contributions liées à l'artillerie dans le terme $E_{C\text{-}Art}$, les contributions liées aux unités robotisées terrestres $E_{C\text{-}UGV}$, les contributions liées aux unités robotisées aériennes (drones, essaims, munitions flottantes) $E_{C\text{-}UAV}$, les contributions liées aux vaisseaux robotisés de surface et sous-marins $E_{C\text{-}USV}$. Les contributions liées aux systèmes de guerre électronique (brouillage, déception électronique, leurres électromagnétiques) interviennent dans $E_{C\text{-}ELEC}$, les contributions cyber offensives et défensives $E_{C\text{-}CYBER}$, les contributions liées au renseignement $E_{C\text{-}RENS}$. L'énergie globale s'écrit Ec = $E_{C\text{-}Art}$ + … + $E_{C\text{-}UGV}$ + $E_{C\text{-}UAV}$ + $E_{C\text{-}USV}$ + $E_{C\text{-}ELEC}$ + $E_{C\text{-}CYBER}$ + $E_{C\text{-}RENS}$ Les intensités catégorielles sont calculées en restreignant les calculs aux contributions des systèmes d'armes correspondants : $I_{C\text{-}Art}$, … , $I_{C\text{-}UGV}$, $I_{C\text{-}UAV}$, $I_{C\text{-}USV}$, $I_{C\text{-}ELEC}$, $I_{C\text{-}CYBER}$, $I_{C\text{-}RENS}$. Cette catégorisation des intensités permet ensuite de mesurer la prédominance de certains systèmes d'armes par rapport à d'autres et d'analyser quantitativement les puissances engagées.

4 - Intensités robotique et cyber

On considère cette fois les énergies et intensité du combat robotisé sur le cube (ou hypercube) de combat :

$$E_{C\text{-}UGV} \ , E_{C\text{-}UAV} , E_{C\text{-}USV} \ \text{et} \ \ I_{C\text{-}USV} , I_{C\text{-}UGV} \ , I_{C\text{-}UAV} \ ,$$

et les intensité cyber et guerre électronique sur l'hypercube :

$$I_{C\text{-}ELEC} , I_{C\text{-}CYBER}$$

Les équilibres entre ces différentes énergies et intensités conditionnent, pour chaque adversaire, la réussite ou l'échec de l'opération militaire en cours.

La cybersécurité des drones et robots engagés dans le cube de combat, combinée à leurs niveaux d'automatismes (L0, L1,L2,L3,L5,L5 – article RDN 2019) conditionne la réussite ou l'échec de l'opération de chaque participant avec de nouveaux enjeux tactiques :

Swarming : essaims aériens, meutes terrestres, Super Swarm (programme prioritaire de l'US Navy avec l'hypothèse d'une attaque d'un Super essaim de 10 000 à 50 000 agents hétérogènes, aériens légérs, mer surface et sous-marin) contre un porte-avion ou un groupe aéronaval US.
Miniaturisation des UAV, vols en GPS denied, traversée de foret par un essaim, challenges souterrains, etc…
Dans chacun de ces défis technologiques, la dimension cyber est déterminante.

Niveaux d'automatisation du système	L0 Système armé pleinement téléopéré	L1 Système armé dupliquant automatiquement l'action de l'opérateur	L2 Système armé semi-autonome en déplacement et en détection de cibles	L3 Système armé autonome soumis à autorisation de tir	L4 Système armé autonome sous tutelle humaine	L5 Système armé autonome sans tutelle humaine
Opérateur humain associé au système	L'opérateur humain téléopère à distance le système à l'aide d'une interface de pilotage déportée.	L'opérateur humain est augmenté par un système qui l'assiste en dupliquant automatiquement ses actions	L'opérateur humain supervise le système en lui fournissant un plan de route et des indications de cibles.	L'opérateur humain n'intervient que pour donner l'autorisation d'ouvrir le feu sur une cible proposée par le système.	L'opérateur humain peut désactiver et reprendre le contrôle du système pleinement autonome	L'opérateur humain n'a pas la possibilité de reprendre le contrôle du système pleinement autonome
Composante mobile-traction du système	Les déplacements du système sont strictement téléopérés par l'opérateur humain	La composante de traction peut suivre et reproduire les déplacements du superviseur humain via ses capteurs	Le système choisit le meilleur chemin en fonction des indications de localisation fournies par l'opérateur	Les déplacements sont décidés par le système en fonction de sa perception du terrain et de ses objectifs de mission	Les déplacements sont décidés par le système en fonction de sa perception du terrain et de ses objectifs de mission	Les déplacements sont décidés par le système en fonction de sa perception du terrain et de ses objectifs de mission
Composante de détection du système	Les détecteurs du système renvoient des informations à l'opérateur	Les capteurs du système détectent les objets que l'opérateur a détecté.	Les capteurs du système détectent automatiquement les objets et cibles potentielles	Les capteurs détectent et reconnaissent les objets de manière autonome	Les capteurs détectent et reconnaissent les objets de manière autonome	Les capteurs détectent et reconnaissent les objets de manière autonome
Composante de reconnaissance et d'acquisition de cibles	La reconnaissance et l'acquisition des cibles sont exclusivement réalisées par l'opérateur humain	L'acquisition des cibles est identique à celle de l'opérateur humain via le système de visée son arme connecté à celui du système	Le système suggère des objets comme cibles potentielles à l'opérateur humain qui définit les cibles à prendre en compte	L'acquisition de cibles s'effectue de manière automatique ou dirigée via les capteurs du système et ses capacités de reconnaissance.	L'acquisition de cibles s'effectue de manière automatique via les capteurs du système et ses capacités de reconnaissance et d'analyse	L'acquisition de cibles s'effectue de manière automatique via les capteurs du système et ses capacités de reconnaissance et d'analyse
Composante armée du système	Les commandes de tirs du système sont exclusivement actionnées par l'opérateur humain	Le système ouvre le feu sur une cible si et seulement si l'opérateur ouvre le feu sur cette cible	Le système ouvre le feu sur la cible après autorisation du superviseur humain	Le système propose une cible et ouvre le feu après autorisation du superviseur humain	Le système décide de l'ouverture du feu sur la cible qu'il a sélectionné mais peut être désactivé par son superviseur	Le système décide de l'ouverture du feu sur la cible qu'il a sélectionné sans possibilité de désactivation (sauf destruction)

Une rupture stratégique qui implique une mise à jour des doctrines

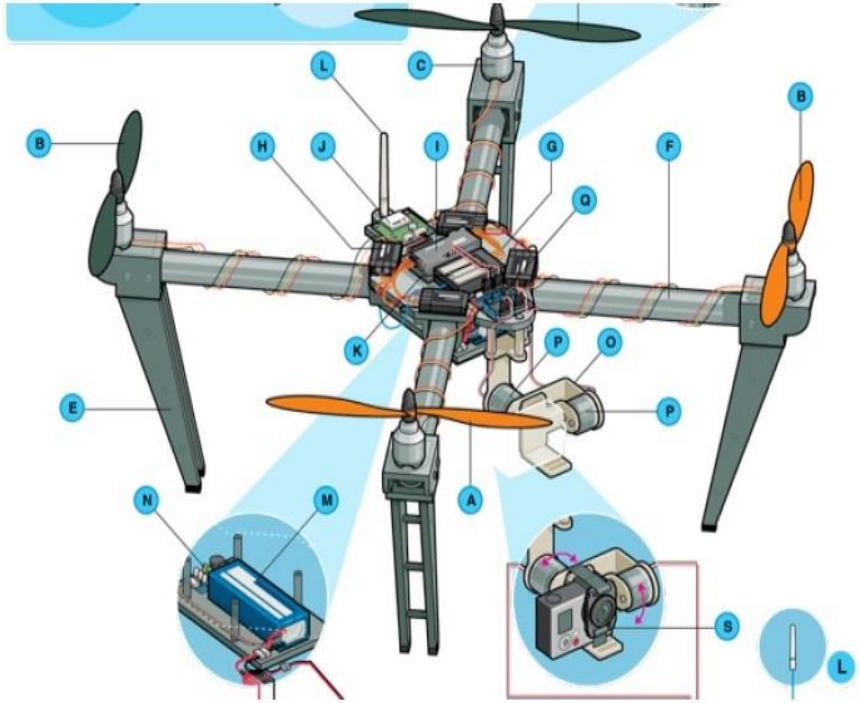
Les drones turcs auraient changé le cours de trois conflits en 2020 ...

Dans son article titré « Les drones, nouvelle arme phare de la défense turque », le quotidien *Le Monde* a indiqué que la Turquie a réorienté son industrie militaire vers la fabrication d'engins sans pilote. Elle exporte de plus en plus de drones. « Auréolés de leurs exploits en Syrie, en Libye et dans le Haut-Karabakh, les drones turcs se vendent comme des petits pains, recueillant un franc succès parmi les pays de l'ancien glacis soviétique » écrit *Le Monde* qui précise que ces drones sont efficaces et bon marché. Il relève que les engins sans pilote turcs ont changé le cours de trois conflits en 2020 en détruisant des chars, véhicules blindés, dépôts de munitions et systèmes de défense antiaérienne de forces adverses. Le quotidien note qu'en moins d'une décennie, la Turquie s'est inscrite parmi les fabricants de drones les plus importants, comme les États-Unis, Israël et la Chine. *Le Monde* décrit le drone *Bayraktar TB2* comme l'engin le plus prisé, précisant qu'il peut récolter des renseignements sur les forces ennemies, diriger les avions de combat vers les cibles et mener ses propres attaques grâce à quatre missiles guidés laser. Le journal souligne dernièrement que les attaques des drones turcs ont paralysé les systèmes anti-aériens russes *Pantsir* en Syrie et en Libye ainsi que les missiles russes *Iskender* en Arménie, et ont ainsi noté des résultats surprenants.

(La voix de la Turquie, le 26-06-2021)

II – Focus sur la cybersécurité des drones aériens légers (UAV)

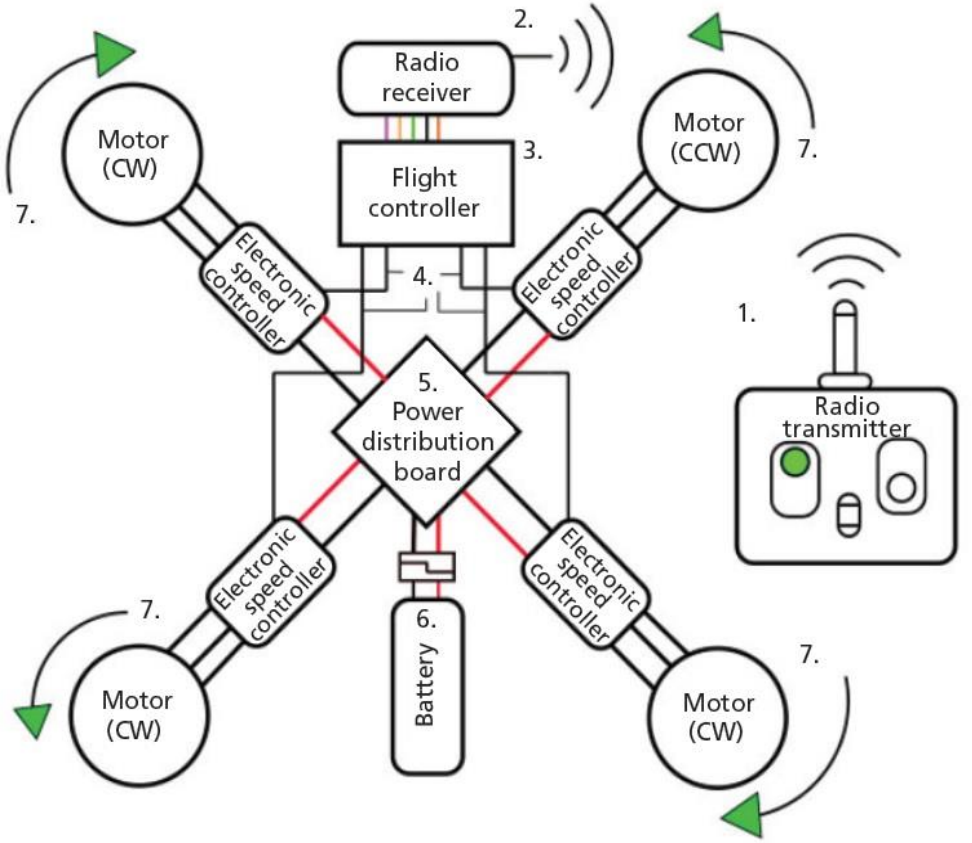
Composant d'un UAV léger



Drone Parts Overview

A. Standard Prop
B. Pusher Prop
C. Brushless Motors
E. Landing Gear
F. Boom
K. Receiver
L. Antenna
M. Battery
N. Battery Monitor
O. Gimbal

Simple Quadcopter Data-Flow Diagram with Single Radio Controller

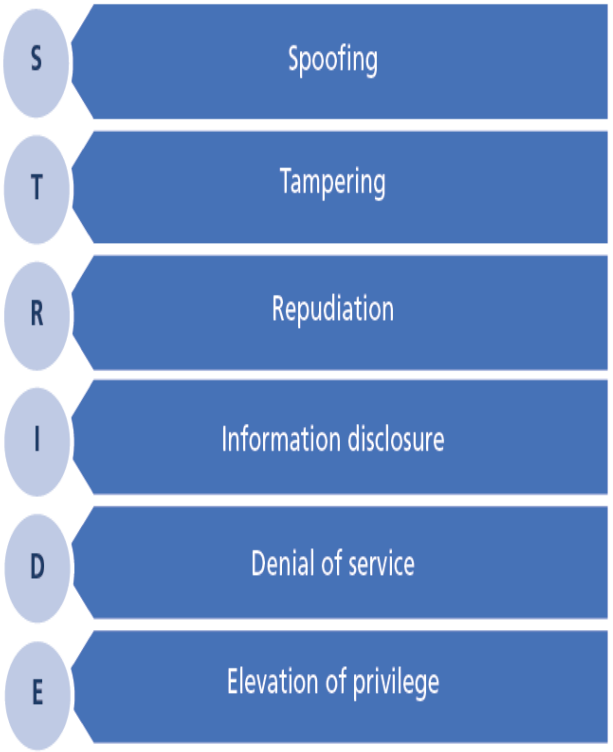


Catégorisation des UAS - dualité Vecteur d'attaque – Cible d'attaque

Categorizing UAS-Related Cyber Threats

	UAS as cyber weapons	UAS as cyberattack targets
DHS/ally UAS	• Disabling adversary networks through local interference • Harvesting adversary credentialing information • Data collection and probing	• Spoofing of law enforcement UAS to misrepresent location information or collected probe data • Take-down, lock-out, or takeover of law enforcement UAS • Theft of UAS identity, network, or collected probe data
Adversarial and other UAS	• Botnet-style stealth network infection enabled by mobile UAS and poorly protected personal WiFi networks • Cascading infection of Internet of Things (e.g., home appliances, lightbulbs, car-charging stations) spread through mobile UAS	• Distorting or destroying collected probe data • Take-down, lock-out, or takeover of adversarial UAS

The STRIDE Threat Taxonomy



Répertorier les risques spécifiques UAV R01 – R14

Risk ID and name

Risk ID	Risk Name	Ref.	Risk ID	Risk Name	Ref.
R01	Fly Away	(1)	R08	Resource Leak	(2)
R02	Loss of GPS	(1)	R09	Battery Depletes	(3)
R03	Loss of Data Link	(1)	R10	Fuel Depletes	(3)
R04	Crash	(1)	R11	Loss of Situational Awareness	(3)
R05	Autopilot Software Error/Fail	(1)	R12	Loss of Direct Visual	(3)
R06	GCS Failure	(1)	R13	Hazard Weather	(3)
R07	Automatic Transmission Locked	(4)	R14	Hostile Environment	(3)

Répertorier les attaques UAV pour matrice risque impact

"Fly away" cyber risk evaluation

Attack ID	Attack Name	Likelihood	Impact	Risk	Acceptability	Recommendation
A18	Man in the middle attack	3	2	6	Tolerable	Mitigate according to best practices
A11	Communication link jamming	3	3	9	Unacceptable	Immediate mitigation required
A19	GPS jamming	3	2	6	Tolerable	Mitigate according to best practices
A20	Replay attack	3	5	15	Acceptable	No action required
A8	Sensor Spoofing	3	2	6	Unacceptable	Immediate mitigation required
A9	Sensor Jamming	3	2	6	Tolerable	Mitigate according to best practices

Répertorier les attaques UAV pour matrice risque impact

Cyber risk assessment matrix

Impact	5	**5A**	**5B**	**5C**	**5D**	**5E**
	4	**4A**	**4B**	**4C**	**4D**	**4E**
	3	**3A**	**3B**	**3C**	**3D**	**3E**
	2	**2A**	**2B**	**2C**	**2D**	**2E**
	1	**1A**	**1B**	**1C**	**1D**	**1E**
		A	B	C	**D**	**E**
		Likelihood				

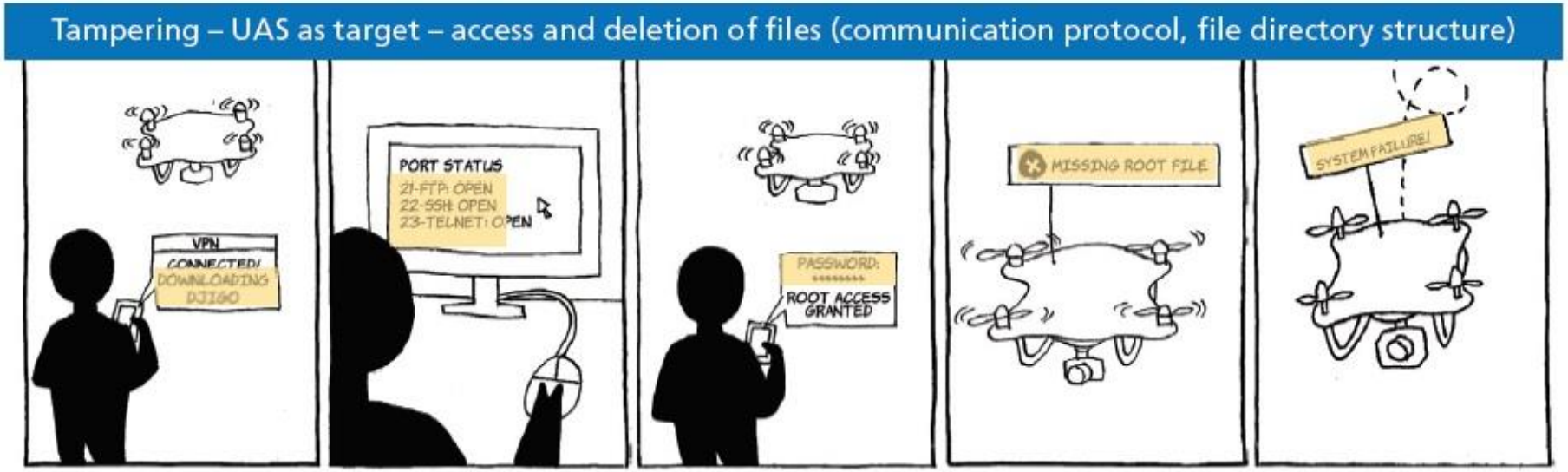
Table provides recommendations according to the acceptability of the likelihood and impact.

Table Interpretation of cyber risk assessment matrix

Acceptability	**Likelihood/impact**	**Recommendation**
Unacceptable	**3-5D and 1E-5E**	Immediate mitigation action and escalation is required. An operational stop should be considered
Tolerable	**4-5A, 3-5B, 1-5C, and 1-2D**	The cyber risk shall be mitigated as low as reasonable practicable and should a formal approval process followed.
Acceptable	**1-3A and 1-2B**	No action required.

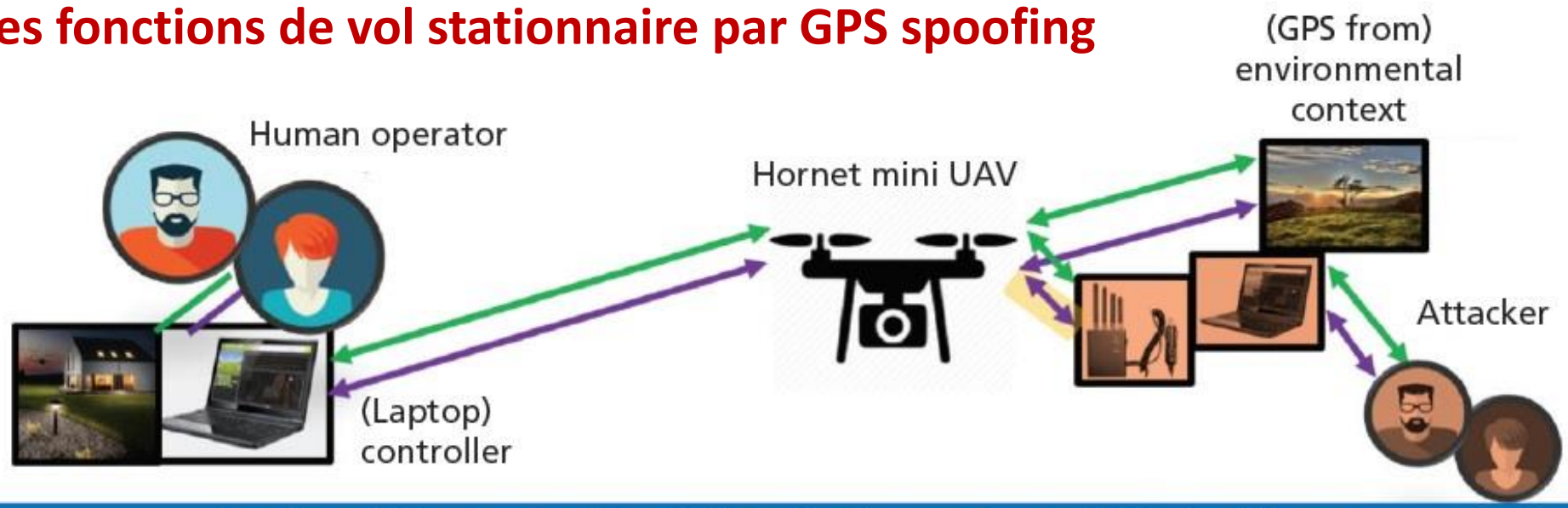
UAS Attack to Access and Delete Files Midflight

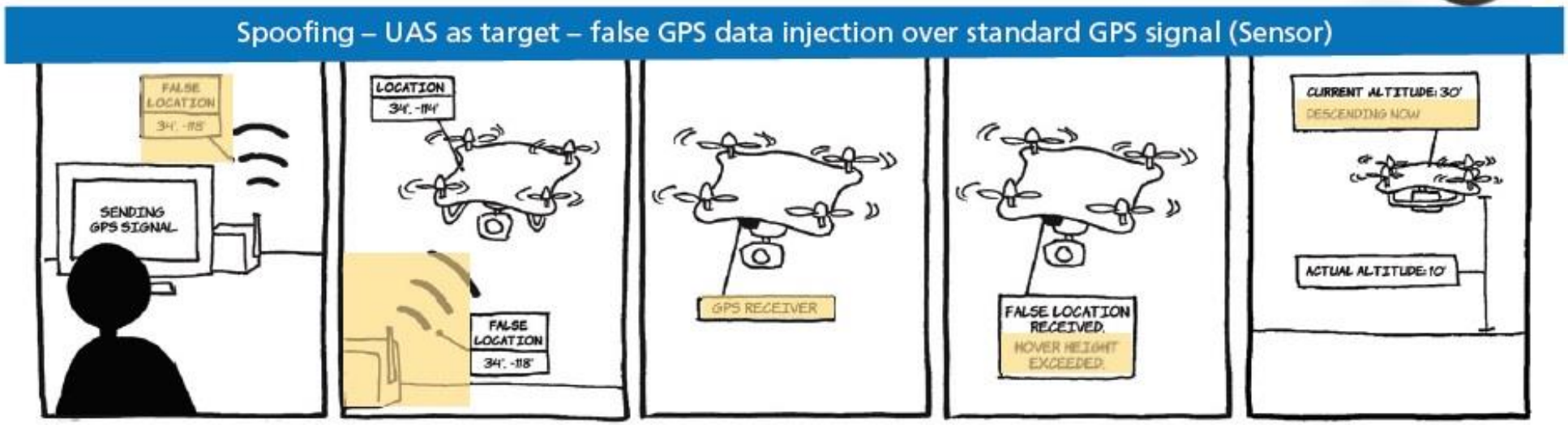
Accès et suppression de fichiers de vol



UAS Attack to Fool Hovering Feature with Spoofed GPS Signal

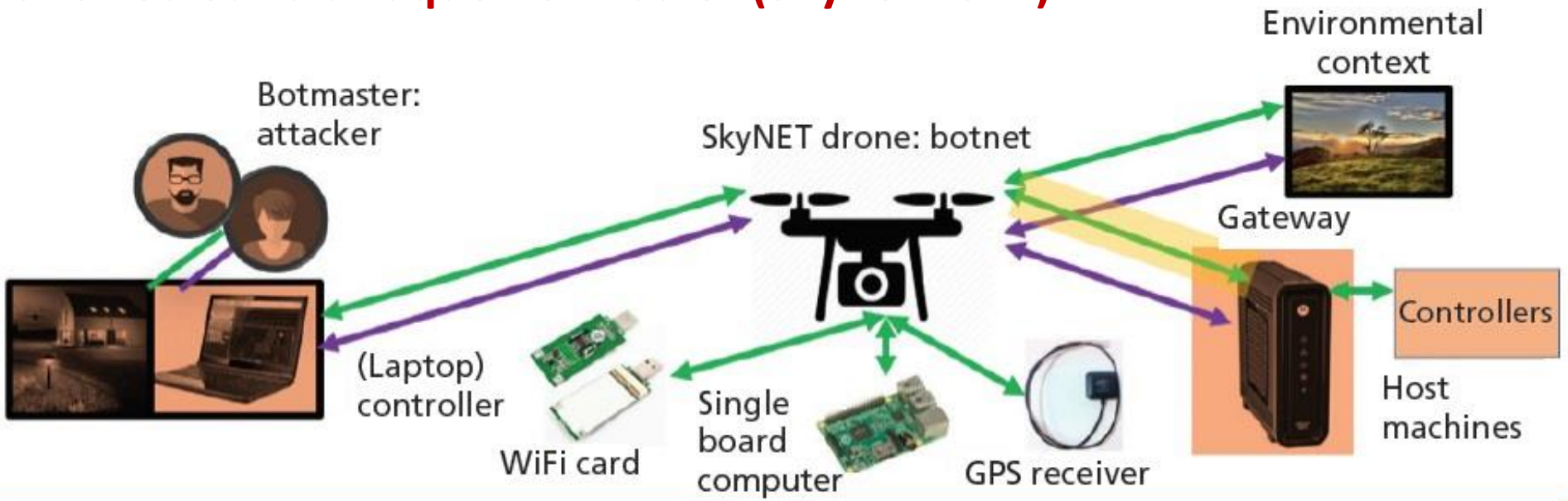
Tromper les fonctions de vol stationnaire par GPS spoofing

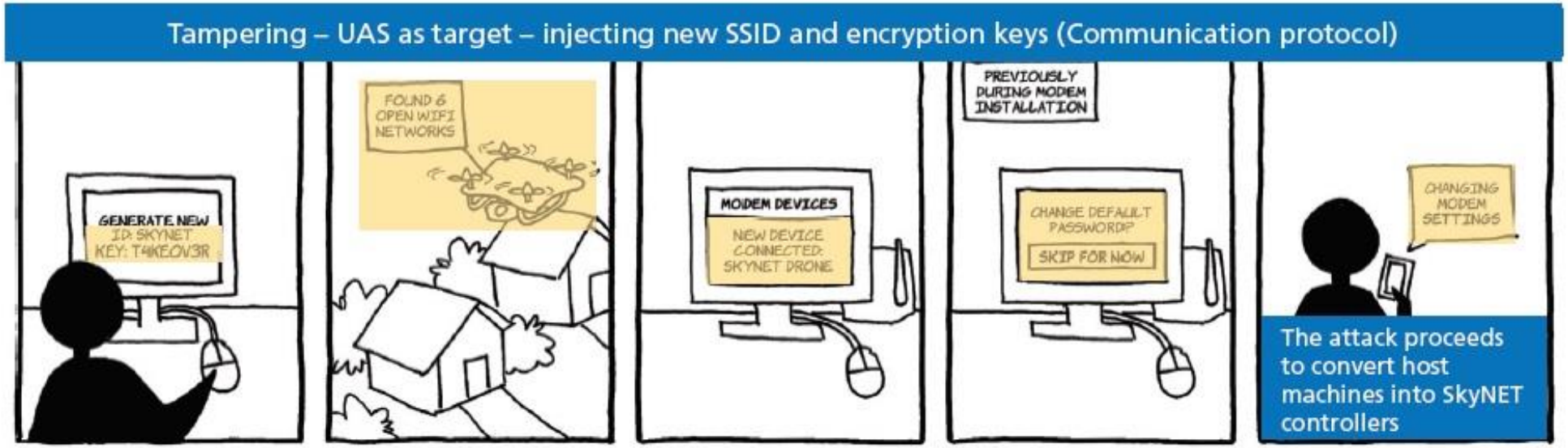




UAS and the Cybersecurity Kill Chain—"UAS as Vector" Exploit (A Drone Botmaster)

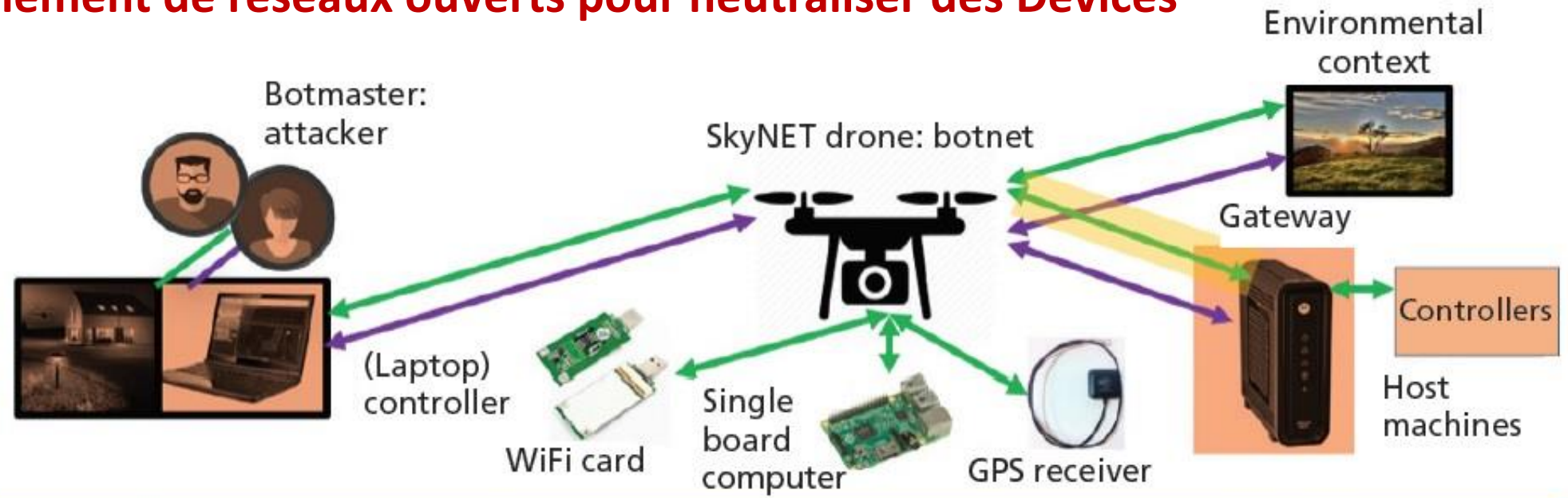
Drone vecteur d'attaque BotMaster (Skynet 2011)

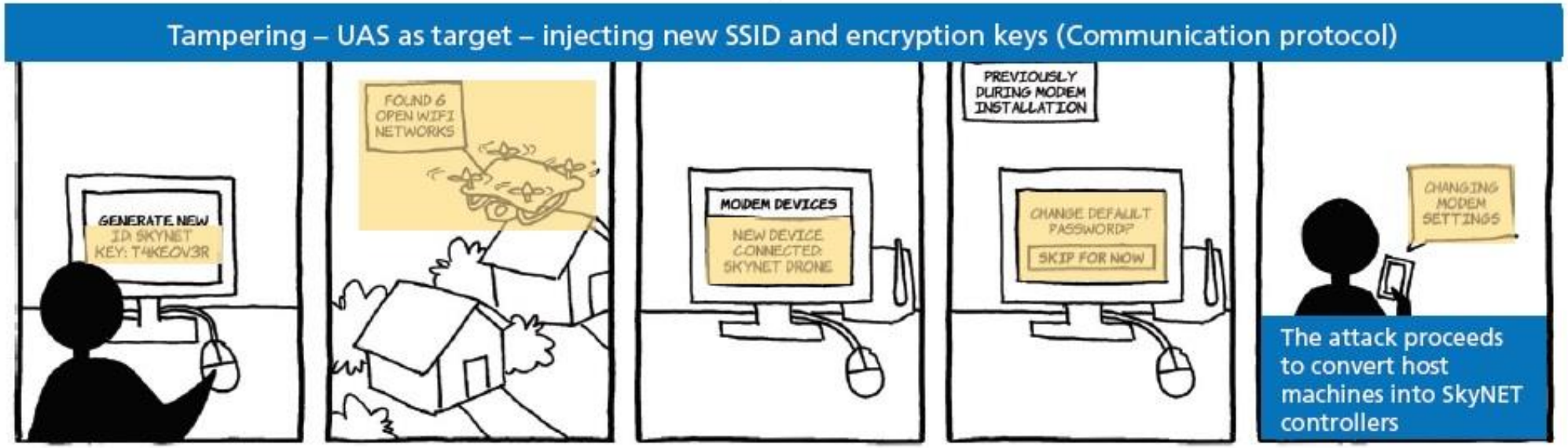




Attack by Drone Hijacks Open Networks and Overrides Networked Devices

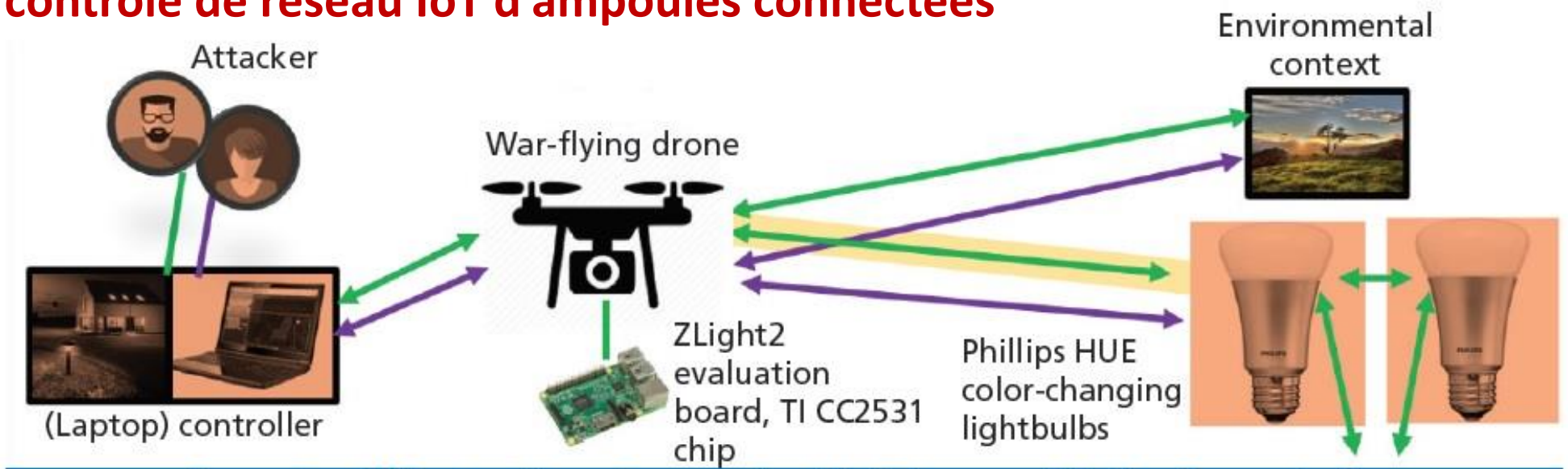
Détournement de réseaux ouverts pour neutraliser des Devices



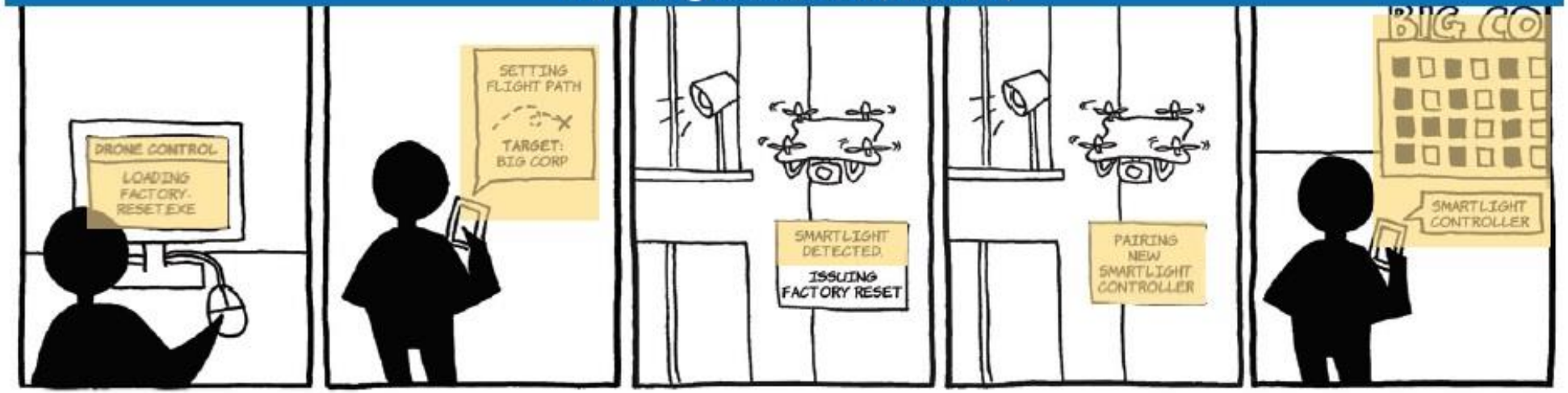


Attack by Drone to Overcome Proximity-Based Control of Smart Lightbulbs

Prise de contrôle de reseau IoT d'ampoules connectées



Tampering – UAS as target – send message "reset to factory new status" and beacon to join drone's zigbee network (firmware)



Références

[1] Cybersecurity Risk assessment for Unmanned Aircraft Systems
https://www.theses.fr/2021GRALT004
https://tel.archives-ouvertes.fr/tel-03200719