Renseignement humain à l'ère post-numérique

Quand l'espionnage adopte le modèle de la prestation de service

L'externalisation des opérations de renseignement et de sabotage vers des « agents à la tâche » n'est pas une anomalie conjoncturelle : c'est une réponse rationnelle d'acteurs hostiles à la double contrainte de l'**attribution** et de la **judiciarisation**. Deux affaires récentes en donnent la matrice ; une série d'incidents européens montre qu'elle vise déjà, directement, les entreprises.

OSINT PROTECT

OSINT Protect: Renseignement Sécurisé & Veille Stratégique | OSINT PROTE...

OSINT Protect se spécialise dans le renseignement sécurisé par sources ouvertes, aidant les entreprises à identifier les menaces numériques et à protéger leur patrimoine. Nos...

Deux affaires qui posent le modèle

Deux cas judiciaires récents — l'un en Inde, l'autre en Allemagne — cristallisent la logique opérationnelle du nouvel espionnage externalisé.

🇮🇳 Réseau Bhatti — Inde / ISI

Des recrues sans engagement politique fort — hommes de 20 à 30 ans, petits commerçants en détresse financière — sont approchées via comptes anonymes et messageries chiffrées (WhatsApp, Signal). Elles exécutent des **micro-tâches tarifées** : propagande, repérage de cibles, transport d'armes par « dead drop », jusqu'aux contrats d'assassinat. Chaque maillon ignore le reste du dispositif. La motivation est strictement **transactionnelle**.

🇩🇪 Procès OLG Stuttgart — 18 août 2026

Trois ressortissants ukrainiens, recrutés par un organisme russe, expédient des colis munis de **traceurs GPS** pour cartographier délais et itinéraires postaux — reconnaissance préparatoire à des envois incendiaires. Un seul condamné, à un an et trois mois déjà couverts par la détention provisoire. Les deux autres acquittés : la cour n'a pu établir qu'ils connaissaient le plan d'ensemble. Le terme allemand dit tout : ***Wegwerf-Agenten*** — agents jetables.

L'acquittement de Stuttgart n'est pas un échec de la justice : c'est la **performance attendue du dispositif**, qui optimise sciemment l'écart entre le seuil d'intentionnalité qu'exige le droit pénal et l'ignorance organisée de l'exécutant.

Le secteur privé est déjà le champ de bataille

La même mécanique frappe, depuis 2024, des **cibles strictement privées en Europe**. Ce ne sont pas des symboles étatiques qui ont été visés, mais des actifs commerciaux choisis pour leur signature géopolitique ou leur valeur de démonstration.

1

Mars 2024 — Entrepôt Leyton, Londres

Un entrepôt abritant de l'aide humanitaire et des équipements Starlink destinés à l'Ukraine est incendié sur ordre du groupe **Wagner** (~1 M£ de dégâts). Le montage est un cas d'école de cloisonnement : les trois exécutants ignoraient travailler pour Wagner. Premières peines sous le *National Security Act 2023* — jusqu'à 17 ans pour le recruteur Dylan Earl.

2

Juillet 2024 — Colis incendiaires DHL, Leipzig & Birmingham

Un dispositif au magnésium dissimulé dans un faux appareil de massage, parti de Vilnius, provoque un incendie au centre de tri DHL de Leipzig. Un colis quasi identique prend feu à Birmingham la même semaine. Les services occidentaux y ont vu des **opérations d'essai** avant d'éventuelles cibles nord-américaines.

3

Mai 2024 — Centre commercial Marywilska 44, Varsovie

Le plus grand centre commercial de la capitale polonaise est détruit par incendie. Officiellement attribué en 2025 par le Premier ministre Donald Tusk aux **services de sécurité russes**. Les incendiaires — souvent des immigrés ukrainiens ou biélorusiens — avaient été recrutés en ligne et payés à la tâche.

4

Juillet 2024 — Projet d'assassinat visant Armin Papperger (Rheinmetall)

Les renseignements américain et allemand déjouent un projet d'assassinat ciblant le PDG de Rheinmetall, fournisseur d'armes de Kyiv. **La cible n'est plus un site, mais un dirigeant** — pour ce qu'il représente géopolitiquement.

Analyse du mode opératoire

Pas une rupture : un passage à l'échelle

L'agent à usage unique n'est pas une invention numérique. Les services de la Guerre froide connaissaient déjà le *throwaway*. Ce qui est neuf n'est pas le principe mais son **industrialisation**, rendue possible par trois infrastructures civiles :

📱 Plateformes de recrutement

Un vivier de désœuvrés transformé en marché de sous-traitance à la demande

₿ Cryptomonnaies

Dissolution de la traçabilité financière ; paiement anonyme et irréversible

📦 Logistique commerciale

La chaîne d'approvisionnement civile, tour à tour capteur de reconnaissance et vecteur d'attaque

Ce qu'un État achète réellement

Ce n'est pas d'abord une **capacité de sabotage** — il en dispose. C'est du **déni plausible**.

Le cloisonnement, le paiement en crypto, le recruteur sous pseudonyme ne sont pas des maladresses : ce sont les **caractéristiques du service vendu**.

Le système est conçu pour produire des acquittements. Poursuivre l'exécutant interchangeable, c'est jouer le jeu de l'adversaire.

Le levier stratégique se situe aux rares nœuds **non remplaçables** de la chaîne : le recruteur, le point de bascule commanditaire → exécutant, le rail de paiement.

Scénario prospectif : l'automatisation de l'orchestration

Ce scénario n'est pas une prédiction — c'est le prolongement logique de ce qui est déjà jugé. Deux déplacements sont à anticiper.

Recrutement automatisé

Un agent conversationnel, sans handler humain, sélectionne un candidat sur son empreinte sociale, lui confie une micro-tâche « anodine » — photographier un poste de transformation, déposer un paquet — le rémunère en stablecoin. L'exécutant ne voit qu'un employeur numérique de plus.

Attribution quasi impossible

L'ignorance de l'exécutant devient totale. Faute d'un être humain à remonter côté commanditaire, l'attribution judiciaire se heurte à un mur structurel. Le droit pénal, conçu pour l'intentionnalité humaine, se retrouve face à une chaîne entièrement déniable.

Extension des cibles

Après la défense et la logistique : opérateurs de centres de données, sous-traitants d'un réseau d'eau ou d'énergie, PME industrielle avec un contrat sensible. Une reconnaissance confiée à un livreur, un « incident » électrique déclenché par un intérimaire — aucun geste ne suppose de conviction idéologique.

⚠ Tout maillon humain **accessible et précaire** — intérimaire, agent de nettoyage, livreur — constitue un vecteur d'attaque potentiel. L'entreprise n'a pas le luxe d'attendre que la chaîne soit remontée.

Conduites à tenir pour le secteur privé

La première mesure est **cognitive** : admettre que l'on peut être une cible pour ce que l'on *représente*, et non pour ce que l'on a fait. Toute entreprise dont l'activité porte une signature géopolitique doit intégrer la menace hybride à sa modélisation. C'est un changement de posture avant d'être un budget.

🏭 Sûreté physique & logistique

Criblage du courrier et des livraisons, traçabilité de la chaîne de garde, détection d'anomalies à l'entrée. Vidéo-analyse orientée vers les comportements de repérage (photographie insistante, rôdeurs, drones). Suppression incendie renforcée et exercices de continuité d'activité. L'attaque de sabotage reste fruste — donc **détectable**.

👤 Terrain humain — l'angle le plus sous-estimé

L'exécutant recruté, c'est potentiellement votre intérimaire, votre prestataire de nettoyage, votre agent de sécurité — un **« insider par la tâche »** sans histoire d'espion. Criblage sérieux des personnels temporaires, sensibilisation au recrutement par messagerie sous couvert d'un « petit boulot », et canal de signalement simple pour tout salarié sollicité en ligne.

📡 Détection & escalade vers l'État

Traiter les signaux faibles comme du renseignement : micro-paiements atypiques, colis anormaux, repérages suspects. Le rôle de l'entreprise n'est pas d'attribuer — c'est celui de l'État — mais de **détecter, consigner et escalader** rapidement (en France : liaison DGSI et référent sûreté préfectoral).

👔 Protection des dirigeants exposés

Protection rapprochée des dirigeants géopolitiquement exposés, réduction de leur empreinte numérique, sûreté des déplacements. L'affaire Papperger établit que **la cible peut être une personne**, choisie pour ce qu'elle symbolise.

⚖️ Vigilance juridico-assurantielle

Un sinistre qualifié d'acte de sabotage étatique peut tomber sous une clause d'exclusion « guerre » ou « acte de puissance étrangère hostile ». **Relire les polices**, négocier le périmètre, bâtir un plan de crise traitant d'emblée un incident comme possiblement commandité — attribution, communication, continuité — plutôt que comme simple accident.

La coopération européenne et l'harmonisation pénale restent aujourd'hui davantage un vœu qu'une réalité opérationnelle. L'exécutant que l'on juge n'est jamais la cible que l'on cherche.