SÉVERINE MEUNIER

Experte en Sécurité Numérique et Intelligence Appliquée

L'INTELLIGENCE ARTIFICIELLE AU SERVICE DU CRIME ORGANISÉ : L'EUROPE FACE À UN DILEMME STRATÉGIQUE

L'INTELLIGENCE ARTIFICIELLE N'EST PLUS UN SIMPLE ACCÉLÉRATEUR ÉCONOMIQUE : ELLE EST DEVENUE UN MULTIPLICATEUR OPÉRATIONNEL POUR LE CRIME ORGANISÉ.

Mais en Europe — et singulièrement en France — répondre avec les mêmes outils se heurte à des garde-fous juridiques et éthiques stricts. Entre efficience criminelle et respect des droits fondamentaux, comment concilier sécurité et démocratie ?

CONTEXTE : L'IA COMME CATALYSEUR DU CRIME ORGANISÉ

Les organisations criminelles exploitent aujourd'hui l'IA pour automatiser des fraudes, créer des contenus falsifiés et optimiser la logistique de leurs trafics. Des deepfakes aux systèmes de phishing ultra-personnalisés, en passant par l'automatisation de circuits financiers opaques, la technologie devient un multiplicateur de capacités pour des réseaux qui opèrent à l'échelle mondiale. Europol et d'autres instances internationales alertent sur la vitesse et l'efficacité de ces nouveaux modes opératoires.

Contrairement à certaines représentations, l'usage criminel de l'IA ne transforme pas les trafics classiques — drogues, traite, contrefaçon, contrebande — qui demeurent majoritairement analogiques. La véritable évolution se situe dans les marges financières : fraude, escroqueries, faux ordres, détournements, micro-blanchiment.

Ces segments, plus discrets mais stratégiques, absorbent aujourd'hui l'essentiel des innovations liées à l'IA. C'est sur cette composante "crime économique", souvent sous-estimée, que repose désormais une part croissante du financement des organisations criminelles.

L'IA transforme le crime organisé en une machine agile et adaptative, capable d'opérer plus vite que la plupart des institutions publiques.

L'IA ne crée pas un crime organisé augmenté : elle amplifie le crime organisé déjà rentable.

ÉTAT DES LIEUX : COMMENT LES RÉSEAUX CRIMINELS « APPRENNENT » ET AGISSENT

1. **Phishing et fraude automatisés :**
   L'IA permet de générer des messages multilingues hyper-personnalisés, testés et ajustés en continu selon les réponses des victimes.
2. **Faux identitaires et extorsion :**
   La génération audio et vidéo facilite les usurpations de voix ou de visages à des fins d'extorsion ou de chantage.
3. **Blanchiment sophistiqué :**
   Les modèles d'IA orchestrent des chaînes financières complexes, avec comptes factices et micro-transferts, rendant le suivi des fonds difficile.
4. **Adaptation tactique en temps réel :**
   Grâce à l'IA et à l'analyse OSINT, les réseaux ajustent leurs actions en fonction des mesures de police ou des fermetures de plateformes.

DES CHIFFRES CONFIRMENT CETTE DYNAMIQUE :

EPPO: 2 666 enquêtes en cours pour 24,8 milliards d'euros de préjudice, dont 13,15 milliards liés aux fraudes à la TVA. https://www.eppo.europa.eu/en/media/news/2024-annual-report-eppo-leading-charge-against-eu-fraud

OLAF: 871,5 millions d'euros de fonds détournés identifiés et 43,5 millions d'euros de dépenses frauduleuses évitées. https://anti-fraud.ec.europa.eu/media-corner/news/olaf-exposes-fraud-involving-over-eu870-million-2025-06-16_fr

Ministère de l'Intérieur: 348 000 atteintes numériques enregistrées, dont 226 300 atteintes aux biens, principalement des escroqueries. Source : Ministère de l'Intérieur, janvier 2025

https://www.interieur.gouv.fr/actualites/communiques-de-presse/publication-du-rapport-annuel-relatif-a-cybercriminalite

Ces données confirment une tendance profonde : la fraude est devenue un moteur financier majeur, stable et peu risqué pour les organisations criminelles, bien plus que certains trafics traditionnels.

Ces tendances montrent que l'IA n'est pas seulement un outil : elle va devenir une compétence stratégique pour le crime organisé.

Le futur du crime est moins technologique qu'adaptatif : l'IA accélère ce qui fonctionnait déjà.

MODE OPÉRATOIRE : UNE ORGANISATION NUMÉRIQUE ET MODULAIRE

Les réseaux criminels structurent désormais leurs activités comme de véritables chaînes de production numériques :

- **Spécialisation des rôles :**
  développeurs de malware, opérateurs de comptes, gestionnaires de marketplaces illicites.
- **Exploitation des vulnérabilités des systèmes :**
  manipulation de données ou attaques sur des modèles d'IA pour contourner les défenses.
- **Réactivité accrue :**
  adaptation rapide aux mesures des forces de l'ordre grâce à l'analyse automatisée de données ouvertes.

Cette modularité confère aux organisations criminelles une résilience opérationnelle et un avantage stratégique difficile à contrer avec les méthodes traditionnelles.

Au-delà de la seule modularité, l'IA renforce la capacité des réseaux à exploiter des « signaux faibles » : comportements atypiques, réactions émotionnelles, horaires de réponse, traces OSINT.

Loin d'un mythe technologique, il s'agit d'une optimisation incrémentale : tester, mesurer, ajuster. Cette logique quasi-industrielle n'augmente pas la criminalité en volume, mais en efficience, rendant certains schémas d'escroquerie plus difficiles à détecter pour les dispositifs de conformité.

Le crime organisé ne devient pas numérique : il devient hybride. Et c'est pire.

>>>

>>> LE DILEMME EUROPÉEN ET FRANÇAIS : POURQUOI NOUS NE POUVONS PAS « JOUER LE MÊME JEU »

En Europe, et en France en particulier, les autorités font face à un paradoxe : elles disposent de moyens légaux et techniques limités pour utiliser l'IA à des fins offensives ou d'infiltration.

CONTRAINTES MAJEURES

- **Réglementation sur l'IA (AI Act) :** interdiction de certaines manipulations et limitations strictes pour la surveillance automatisée.
- **Protection des données (GDPR) :** encadrement rigoureux de la collecte et du traitement des informations personnelles.
- **Cadres procéduraux stricts :** création de faux profils ou infiltration de forums illicites nécessite autorisation judiciaire.
- **Culture démocratique et droits fondamentaux :** toute action intrusive doit être proportionnée et contrôlée, sous peine de rendre les preuves irrecevables.

Ces contraintes limitent l'usage de certaines armes technologiques que les criminels utilisent sans scrupules, créant un décalage tactique significatif

CRIMINALITÉ ANALOGIQUE

Une part importante du crime organisé continue pourtant de prospérer par des moyens strictement analogiques : transport physique, messageries humaines, réseaux relationnels, comptabilité hors-système. Comme le rappellent de nombreux praticiens, "le meilleur moyen d'échapper à la surveillance numérique reste de ne pas être numérique". La sophistication technologique ne concerne qu'une fraction du paysage criminel.

> Le futur du crime est moins technologique qu'adaptatif : l'IA accélère ce qui fonctionnait déjà.

PARADOXE EUROPEEN

L'Europe a développé le meilleur cadre éthique du monde… mais pas la meilleure vitesse d'exécution.

■ **L'enquêteur Quentin Mugg ancien enquêteur à l'OCRGDF et auteur de Argent sale : la traque, le rappelle dans plusieurs de ses travaux :** les courtiers criminels demeurent depuis des décennies les véritables moteurs invisibles du blanchiment, bien plus que les innovations technologiques récentes. Il décrit cette hégémonie discrète, fondée sur des réseaux de confiance, des flux non bancarisés et des systèmes comme le Hawala, qui continuent de fonctionner parfaitement en marge de toute surveillance numérique.

Ce contraste souligne un point essentiel : l'IA renforce la fraude observable, mais une large partie des flux criminels reste invisible par nature, non pas par technologie.

Mais l'enjeu principal n'est pas technologique : il est écosystémique.

L'IA n'invente pas le crime. Elle optimise un système qui existe déjà depuis longtemps, structuré par des réseaux d'intermédiaires qui maîtrisent l'art de la discrétion et de l'exploitation des failles.

L'essor de l'intelligence artificielle bouleverse profondément les modes opératoires du crime organisé. Loin des représentations classiques centrées sur la violence, les armes ou les marquages territoriaux, la criminalité contemporaine s'appuie désormais sur une logique industrielle, fondée sur la donnée, l'automatisation et l'externalisation. L'IA devient un levier, un amplificateur et, de plus en plus, un architecte invisible des attaques numériques, des fraudes massives, de la pédocriminalité en ligne ou du blanchiment financier.

■ **Au cœur de cette transformation se trouve une réalité encore trop peu comprise :** l'économie criminelle repose moins sur ses exécutants que sur ses facilitateurs. Ce ne sont pas les profils voyants qui structurent l'écosystème, mais ceux qui orchestrent, conseillent, anonymisent, connectent, forment, optimisent. Ces intermédiaires — brokers, développeurs, logisticiens, blanchisseurs, ingénieurs IA — façonnent l'infrastructure du crime moderne.

■ **Parmi eux, une catégorie se distingue par son ancienneté et son rôle déterminant :** les "courtiers criminels". Comme le rappelle un article récent du Nouvel Obs, ces acteurs n'ont rien d'un phénomène émergent : ils constituent depuis des décennies la charpente silencieuse de la criminalité organisée. Leur fonction n'est pas de prendre des risques, mais de rendre le système fluide, rentable et surtout invisible.

LES COURTIERS CRIMINELS : UNE HÉGÉMONIE SILENCIEUSE QUI PRÉCÈDE L'IA

Longtemps ignorés des politiques publiques, les courtiers criminels opèrent dans l'ombre comme les véritables ingénieurs de résilience du crime organisé. Leur rôle s'étend bien au-delà du blanchiment traditionnel :

- Ils assurent la circulation et la conversion des flux illicites ;
- Ils connectent les groupes entre eux ;
- Ils fournissent l'infrastructure logistique, technique et financière dont les criminels ont besoin ;
- Ils opèrent à la frontière du légal et de l'illégal, exploitant les angles morts réglementaires.

Ils préexistent à l'IA, mais l'IA démultiplie leur puissance. Elle leur offre une capacité nouvelle à :

- Cartographier automatiquement les vulnérabilités d'un système ;
- Industrialiser des escroqueries à grande échelle ;
- Automatiser la création d'identités synthétiques, de contenus prétextes ou de deepfakes crédibles ;
- Diversifier les flux financiers en s'appuyant sur des intermédiaires dématérialisés ;
- Faciliter l'exploitation sexuelle des mineurs en ligne via des outils de diffusion et de camouflage.

L'IA devient ainsi l'outil parfait pour un intermédiaire discret : un multiplicateur d'efficacité sans exposition.

"Les courtiers criminels restent l'infrastructure la plus résiliente du blanchiment : aucune IA ne concurrence un système qui n'a jamais été numérique prospérer sans être vu."

Comparaisons internationales

- **Royaume-Uni :**
  le cadre CHIS (Covert Human Intelligence Sources) autorise sous supervision l'infiltration, offrant plus de marges de manœuvre.
- **États-Unis :**
  moins de restrictions sur l'expérimentation, avec des agences capables d'« active defense » mais sous débats sur les droits civiques.
- **Japon :**
  législation d'active cyberdefence permettant des actions proactives sur infrastructures adverses.

En comparaison, l'Europe favorise la protection des droits et la transparence, mais au prix d'une prudence qui réduit sa capacité à contrer rapidement l'IA malveillante.

Propositions : réduire le déséquilibre tout en respectant l'État de droit

1. **Mandats IA spécialisés :**
   autorisations judiciaires encadrées pour certaines opérations IA ciblées, avec durée et périmètre limités.
2. **Sandboxes techniques :**
   environnements sécurisés pour tester des modèles IA en conditions contrôlées, en partenariat public-privé.
3. **Centres d'expertise IA-forensics :**
   analystes, data scientists et juristes formés pour investigations techniques légales.
4. **Coopération internationale renforcée :**
   partage d'indicateurs et outils forensiques en temps réel.
5. **Outils de détection partagée :**
   bases d'IOCs, détection de deepfakes, watermarking vérifiable pour neutraliser les campagnes criminelles.
6. **Expérimentations légales pilotes :** infiltration passive de forums ou tests encadrés de détection de fraudes IA pour évaluer l'efficacité avant généralisation.

Ces mesures permettent de réduire l'écart technologique avec les criminels tout en respectant la législation et les principes démocratiques.

CONCLUSION PROSPECTIVE

Même si Le crime organisé maîtrise l'IA — c'est un fait. L'IA ne reconfigure pas encore le crime organisé : elle amplifie surtout la composante frauduleuse, celle qui s'appuie sur des flux officiels, des identités légitimes et des comportements détectables.

Le cœur des trafics, lui, demeure encore fondamentalement humain, relationnel, territorial.

L'Europe et la France doivent répondre de manière proactive, mais encadrée, pour ne pas laisser un avantage stratégique aux contrevenants. La solution réside dans l'adaptation des cadres légaux, le développement de capacités techniques spécialisées et la coopération internationale.

L'Europe peut protéger ses citoyens tout en restant fidèle à ses principes : sécurité, transparence et respect des droits fondamentaux

Le véritable enjeu stratégique pour l'Europe consiste donc à anticiper les usages criminels en testant des solutions encadrées et, à absorber cette criminalité financière augmentée, tout en continuant à surveiller des réseaux analogiques qui échappent entièrement au numérique. Cette double vigilance sera déterminante pour préserver sécurité, état de droit et équilibre démocratique.. ■