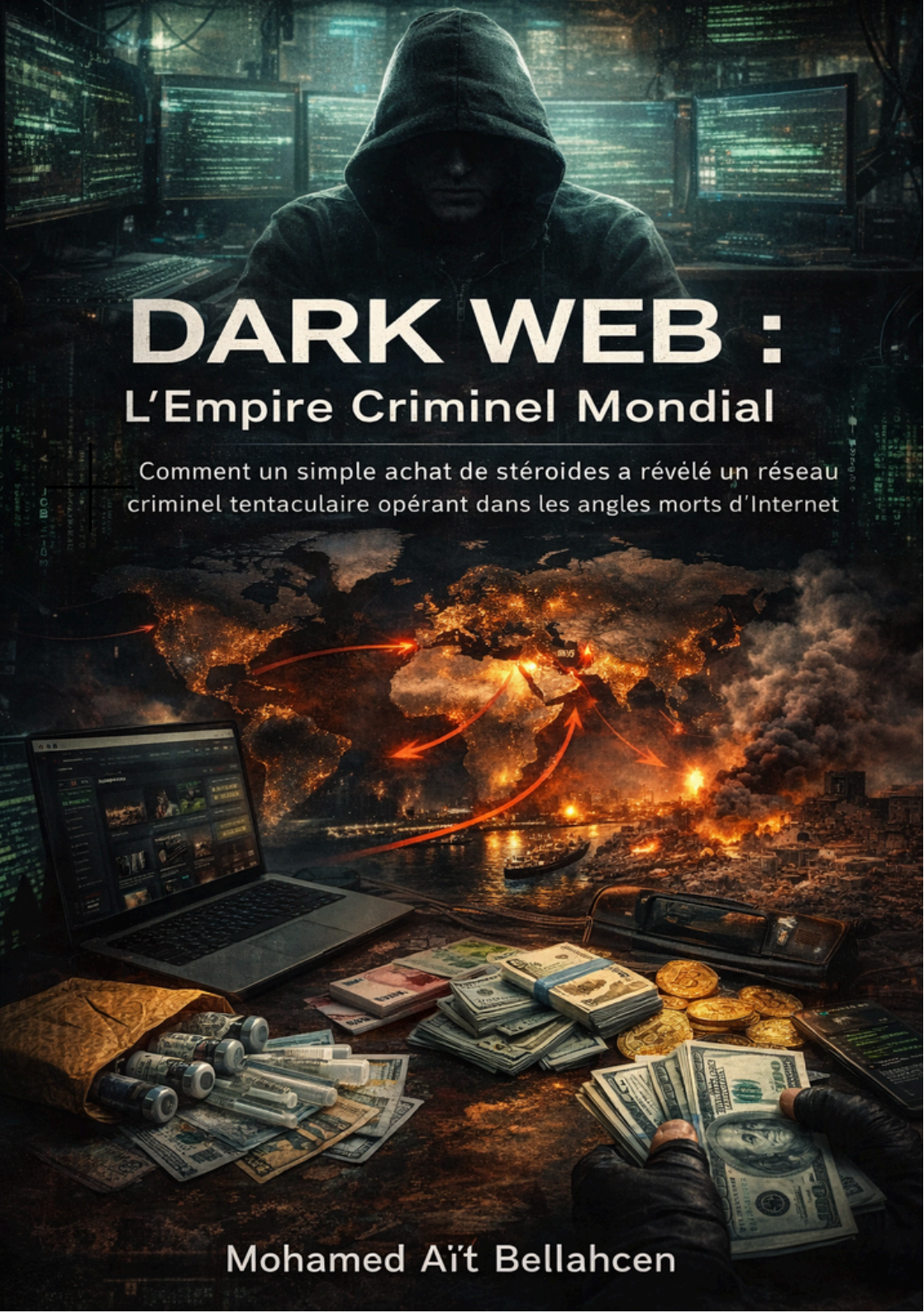
DARK WEB :
L'Empire Criminel Mondial
Comment un simple achat de stéroides a révélé un réseau criminel tentaculaire opérant dans les angles morts d'Internet
Mohamed Aït Bellahcen

À PROPOS DE CE FANZINE

Ce Fanzine est une enquête approfondie et élargie, fondée sur les faits rapportés par l'article original de Mohamed *TAoiut s*B *derlolaithsc reéns epruvébsli é— l e2 012666* mars 2026. Il vise à offrir au lecteur une compréhension complète des mécanismes du Dark Web, de la criminalité numérique transnationale et des enjeux géopolitiques qui en découlent.

TABLE DES MATIÈRES

PARTIE I

Les Faits

Tout commence par un geste banal dans un monde qui ne l'est pas. L'histoire d'Anthony Coronadi est avant tout celle d'un individu ordinaire happé par une mécanique extraordinaire.

CHAPITRE 01

L'Homme Ordinaire et le Colis Fatal

Anthony Coronadi n'est pas un criminel. Du moins,pas au sens classique du terme. C'est un jeune Américain passionné de musculation, sans casier judiciaire, sans réseau mafieux, sans ambition criminelle structurée. Il s'entraîne régulièrement, cherche à progresser plus vite, et un jour, il tape quelques mots sur un moteur de recherche.

Ce qui s'ouvre devant lui n'est pas un simple marché noir de rue. C'est un écosystème numérique sophistiqué, organisé comme un site e-commerce, avec des avis utilisateurs, des garanties de livraison et des prix compétitifs. Les stéroïdes anabolisants qu'il cherche sont là, disponibles, accessibles en quelques clics. Il commande. Il paye en cryptomonnaie. Il attend.

> Le Dark Web compte des milliers de boutiques en ligne. Certaines existent depuis des années, avec des systèmes de notation, de service client et de politique de remboursement.

Le colis arrive. Anthony l'ouvre. Il contient bien ce qu'il a commandé, mais aussi — sans qu'il le sache encore — les preuves d'un réseau international que les forces de l'ordre pistaient depuis des mois.

C'est ce paradoxe qui rend cette affaire si révélatrice de notre époque : le consommateur lambda, celui qui ne cherche qu'un raccourci vers la performance, devient malgré lui le maillon d'une chaîne criminelle mondiale. Sa naïveté numérique n'est pas une excuse légale. Elle est un symptôme sociétal.

La question que pose ce dossier n'est donc pas seulement : *Comment Anthony a-t-il fait ?* Mais surtout : *Pourquoi est-il si facile d'entrer dans ce monde ?*

CHAPITRE 02

Anatomie d'une Commande Illégale

Pourcomprendrecomment unesimple commandede stéroïdes peut déclencher une enquête internationale, il faut disséquer le mécanisme d'achat tel qu'il fonctionne sur le Dark Web.

L'accès au Dark Web nécessite un navigateur spécialisé — le plus connu étant Tor, acronyme de The Onion Router. Ce logiciel fait transiter les données à travers plusieurs serveurs cryptés répartis dans le monde entier, rendant le traçage quasi-impossible pour un observateur extérieur.

Les étapes d'une transaction type :

- Connexion via Tor — l'adresse IP réelle est masquée.
- Navigation sur un marché clandestin avec une adresse .onion.
- Création d'un compte sous pseudonyme avec email jetable.
- Paiement en Bitcoin ou Monero — traçabilité réduite.
- Livraison en adresse neutre ou boîte postale.
- Communication via messagerie chiffrée (PGP).

Ce processus, pensé pour l'invisibilité, comporte pourtant des failles. Une erreur de configuration, un colis intercepté par les douanes, une adresse de livraison liée à une identité réelle : chacun de ces points peut devenir le fil que les enquêteurs tirent pour démêler l'ensemble du réseau.

Dans le cas d'Anthony, c'est précisément ce scénario qui s'est produit. Un colis jugé suspect par les douanes américaines, une adresse de livraison enregistrée, et voilà toute la mécanique judiciaire qui s'enclenche.

CHAPITRE 03

L'Engrenage : de l'Achat à l'Arrestation

L'arrestation d'AnthonyCoronadin'est paslafin d'unehistoire. Elle en est le début. Lorsque les enquêteurs creusent, ils découvrent que son cas n'est qu'un point d'entrée dans un labyrinthe logistique et financier qui s'étend sur trois continents.

Les douanes signalent le colis aux agences fédérales. Une enquête numérique s'ouvre. Les métadonnées de transaction, les adresses Bitcoin utilisées, les patterns de livraison : tout est passé au crible. L'analyse blockchain, technique consistant à retracer les flux de cryptomonnaie, révèle que des milliers de transactions similaires ont transité par les mêmes portefeuilles numériques.

> L'analyse blockchain permet de suivre les cryptomonnaies d'adresse en adresse. Si un portefeuille est un jour lié à une identité réelle — par un échange légal, par exemple — toute la chaîne peut être remontée.

Les enquêteurs identifient rapidement que les colis sont expédiés depuis le Royaume-Uni, plus précisément depuis la région de Coventry. Une adresse y est repérée. Un contact : Amanda. Elle reçoit les marchandises de l'étranger et les réexpédie vers les États-Unis. Elle est, sans le savoir vraiment, une « mule postale ».

Parallèlement, les flux financiers pointent vers l'Inde. Un opérateur — dont le pseudonyme en ligne est « Liston » — semble coordonner l'ensemble. Les agences américaine, britannique et indienne commencent à partager leurs informations. L'enquête devient transnationale.

PARTIE II

Les Acteurs de l'Ombre

Derrièrechaque trafic organisé,il y a des individus. Certains en connaissent les rouages. D'autres n'en voient qu'un fragment. Cette dissociation est la force du système.

CHAPITRE 04

Qui est « Liston » ? Le Fantôme du Réseau

Danstoute enquête criminelled'envergure,ily a unnomqui revient, une identité qui focalise les efforts des enquêteurs sans jamais se laisser totalement saisir. Dans ce dossier, c'est « Liston ».

« Liston » n'est probablement pas un vrai nom. C'est un pseudonyme opérationnel, une façade numérique derrière laquelle se cache soit une personne physique, soit — hypothèse de plus en plus envisagée par les enquêteurs — une structure collective où plusieurs individus partagent les mêmes accès et la même identité numérique.

Ce que l'on sait de « Liston » :

- Il ou elle opère depuis au moins un serveur situé en Inde.
- Les portefeuilles crypto liés à ce pseudonyme totalisent des centaines de millions de dollars.
- Les communications passent par des protocoles PGP avec des clés renouvelées régulièrement.
- Aucune photo, aucun document d'identité vérifiable n'a encore été produit.

L'existence de « Liston » illustre une réalité fondamentale de la criminalité numérique : l'identité peut être une construction permanente, révisable, effaçable. Dans le monde physique, le cerveau d'un réseau laisse des traces : témoins, documents, présence physique. Dans le monde numérique, il peut théoriquement n'exister que comme signal crypté.

Cette invisibilité protège aussi les investisseurs criminels qui financent les opérations sans jamais toucher eux-mêmes à la marchandise. « Liston » est peut-être plusieurs personnes. Peut-être une organisation. C'est là toute la difficulté de la justice à l'ère numérique.

CHAPITRE 05

Amanda et les Mules Humaines

Si« Liston » est l'ombre, Amanda est lalumière du dossier : celle qu'on voit, qu'on identifie, qu'on arrête. Son histoire est celle de milliers de « mules » dans les réseaux criminels modernes.

Amanda est une femme britannique ordinaire. Elle a répondu à une annonce sur internet — une opportunité de travail à domicile. Recevoir des colis, les vérifier, les réexpédier. Une rémunération modeste. Un travail simple.

Elle n'a pas cherché à savoir ce que contenaient les paquets. Ou peut-être qu'elle préférait ne pas le savoir. Ce flou volontaire ou involontaire est précisément ce que les organisateurs exploitent : la plausible dénégabilité des exécutants.

> Le terme « mule » désigne en criminologie toute personne qui transporte ou gère des biens illicites pour le compte d'un réseau, souvent sans en connaître la totalité des enjeux.

Le modèle des mules postales est vieux comme le trafic. Ce qui est nouveau, c'est son industrialisation numérique. Les annonces de recrutement pullulent sur des forums légaux et illégaux. Les candidats sont nombreux : chômeurs, étudiants, personnes en difficulté financière. Le réseau sélectionne, instructs via messagerie chiffrée, paie en cryptomonnaie.

Amanda a été arrêtée. Son cas a permis d'avancer dans l'enquête. Mais des dizaines d'autres « Amandas » existent dans d'autres villes, d'autres pays, réalisant les mêmes gestes sans en mesurer les conséquences.

CHAPITRE 06

Les Architectes Invisibles du Trafic

Entre« Liston » et Amanda,entre lecerveau et lamain, il existe une couche d'acteurs que l'on nomme rarement : les architectes invisibles. Ce sont eux qui font tenir l'ensemble.

Ces acteurs se décomposent en plusieurs catégories fonctionnelles :

Les développeurs

Créent et maintiennent les plateformes du Dark Web, les systèmes de paiement crypté et les outils de communication sécurisée.

Les revendeurs intermédiaires

Achètent en gros et redistribuent via des sous-réseaux locaux, réduisant l'exposition des grossistes.

Les blanchisseurs

Convertissent les cryptomonnaies en monnaies légales via des services de mixage et des exchanges peu regardants.

Les logisticiens

Organisent les routes de livraison, identifient les failles douanières et coordonnent les expéditions.

Les recruteurs

Identifient et enrôlent les mules, les dropshippers et les intermédiaires de toute nature.

Ce qui frappe dans cette organisation, c'est sa ressemblance avec une entreprise légale. Les fonctions sont clairement séparées. La spécialisation est poussée. Il y a même — selon certains rapports d'enquête — des procédures qualité et des systèmes de réclamation.

PARTIE III

L'Anatomie du Dark Web

Pour comprendre l'affaire dans toutesa dimension, il faut comprendre

l'écosystème dans lequel elle s'est développée. Le Dark Web n'est ni un mythe ni une simple abstraction technique.

CHAPITRE 07

Dark Web : Mythes et Réalités

LeDark Webcristallise les fantasmes.Films, séries, journaux : il est souvent dépeint comme un monde parallèle, un gouffre technologique réservé aux hackers et aux criminels. La réalité est plus nuancée — et plus inquiétante.

Les trois couches d'Internet :

Surface Web

Ce que Google indexe. Environ 4% du contenu total d'Internet.

Deep Web

Contenus non indexés : intranets, bases de données, emails, espaces cloud. Représente environ 90% d'Internet.

Dark Web

Sous-ensemble du Deep Web accessible uniquement via des logiciels spéciaux comme Tor. Représente environ 6% du contenu total.

Le Dark Web n'est pas exclusivement criminel. Il abrite des forums de dissidents politiques dans des régimes autoritaires, des journalistes protégeant leurs sources, des lanceurs d'alerte. WikiLeaks y a opéré. Des ONG de défense des droits humains y sont présentes.

Mais il abrite aussi — et massivement — des marchés de trafic. Drogues, armes, données personnelles, faux documents, cyberattaques à la commande. Le volume de transactions illicites y est estimé à plusieurs milliards de dollars annuels.

La puissance du Dark Web ne réside pas dans la technologie seule. Elle réside dans la combinaison de trois facteurs : l'anonymat, la décentralisation, et la monnaie cryptée. Retirez l'un de ces trois piliers et le système s'affaiblit considérablement.

CHAPITRE 08

La Chaîne Logistique du Crime Numérique

L'unedes innovations majeuresdela criminalité numériquemoderne est l'adoption des logiques du commerce en ligne. Le crime organisé s'est mis au e-commerce.

Le modèle opérationnel des marchés du Dark Web ressemble trait pour trait à celui d'Amazon ou d'Alibaba, avec quelques adaptations notables :

- Fiches produits avec descriptions, photos et composition.
- Système d'avis et de notation des vendeurs.
- Service d'escrow (dépôt de garantie) pour sécuriser les transactions.
- Politique de remboursement en cas de non-livraison.
- Support client via messagerie chiffrée.
- Programmes de fidélité et remises pour gros volumes.

Cette professionnalisation du crime a plusieurs conséquences. Elle réduit la barrière à l'entrée pour les consommateurs : nul besoin de connaître un dealer, d'arpenter des rues dangereuses. Elle élargit le marché de façon exponentielle. Elle rend aussi le réseau plus difficile à démanteler : si une plateforme est fermée, une autre émerge en quelques semaines, récupérant vendeurs et clients.

> Silk Road, le premier grand marché du Dark Web, a été fermé en 2013 par le FBI. En moins de six mois, Silk Road 2.0 était opérationnel. Aujourd'hui, des dizaines de plateformes similaires coexistent.

CHAPITRE 09

Cryptomonnaies : L'Argent qui Disparaît

Sile Dark Web est le lieudu trafic, lacryptomonnaie en estle sang. Sans elle, l'essentiel du système s'effondre. Comprendre la finance criminelle numérique suppose de comprendre les mécanismes des actifs cryptés.

Le Bitcoin, créé en 2009, était initialement célébré pour sa transparence : toutes les transactions sont enregistrées sur une blockchain publique. Paradoxalement, c'est cette même blockchain qui en fait un outil ambivalent pour les criminels.

Bitcoin vs Monero : deux approches :

Critère	Bitcoin	Monero
Traçabilité	Transactions visibles	Transactions privées
Adoption légale	Très large	Limitée
Usage criminel	Historique	Croissant
Analyse forensique	Possible	Très difficile

Dans l'affaire Coronadi, les enquêteurs ont saisi des centaines de millions de dollars en Bitcoin. Cette saisie massive a déclenché un conflit diplomatique inédit entre les États-Unis, le Royaume-Uni et l'Inde sur la question de l'attribution et du partage de ces actifs numériques.

PARTIE IV

La Réponse des États

Face àun réseauglobal, mondialisé,technologiquement agile, que peuvent faire des États souverains qui restent fondamentalement territoriaux ?

CHAPITRE 10

Trois Pays, Trois Justices, Un Seul Trafic

L'affaireCoronadimet en scène trois démocraties avec troissystèmes judiciaires distincts, trois cultures légales différentes et, surtout, trois définitions souveraines de ce que signifie « coopérer ».

États-Unis

Systèmecommon law. Priorité à la peine exemplaire. Ressources considérables : DEA, FBI, FinCEN. Tendance à l'extraterritorialité juridique.

Royaume-Uni

Système commonlaw. Approche plus procédurière. La NCA (National Crime Agency) collabore mais reste souveraine. Post-Brexit : moins d'intégration avec Europol.

Inde

Système mixte (common law + droit codifié). Législation sur la cybercriminalité en développement. Sensibilité souveraine élevée sur les données numériques.

Ces trois systèmes convergent sur un même dossier mais avancent à des rythmes différents, avec des règles de preuve différentes et des priorités politiques différentes. L'un veut juger sur son sol. L'autre veut extrader. Le troisième veut garder la main sur les données. Pendant ce temps, le réseau, lui, ne connaît pas de frontières.

CHAPITRE 11

Coopération Internationale : Forces et Limites

Lacoopération judiciaire internationalen'est pas un mythe.Elle existe,elle fonctionne parfois avec efficacité. Mais dans des affaires de cette envergure, ses limites deviennent douloureusement visibles.

Ce qui fonctionne :

- Les échangesd'informations en temps réel via Interpol et Europol.
- Les commissions rogatoires internationales pour accéder aux preuves.
- Les accords bilatéraux d'extradition entre nations partenaires.
- Le partage des analyses blockchain entre agences spécialisées.

Ce qui coince :

- Les délais procéduraux : chaque pays suit ses propres calendriers judiciaires.
- Les conflits de compétence : qui juge en premier ? Qui détient les preuves principales ?
- Les intérêts nationaux divergents sur le partage des actifs saisis.
- L'absence de cadre juridique commun pour les crimes purement numériques.
- Les zones de non-droit : certains pays n'ont pas de traités d'extradition.

L'affaire révèle une vérité inconfortable : la coopération internationale contre la cybercriminalité reste un patchwork d'accords bilatéraux, d'initiatives ad hoc et de bonne volonté politique. Il n'existe pas d'équivalent numérique d'Interpol avec de réels pouvoirs d'action.

CHAPITRE 12

Les Saisies de Bitcoins : Bataille Diplomatique

Quand on parle de criminalité numérique, on parle inévitablement d'argent. Et dans cette affaire, l'argent a pris la forme de centaines de millions de dollars en bitcoins. La question de leur saisie a failli faire dérailler la coopération internationale.

La saisie de cryptoactifs pose des questions inédites :

- Qui détient les clés privées des portefeuilles saisis ?
- Quelle juridiction a compétence pour ordonner la saisie ?
- Comment partager les actifs entre plusieurs États qui ont contribué à l'enquête ?
- Comment valoriser des actifs dont le cours fluctue quotidiennement ?
- Les fonds saisis peuvent-ils être utilisés pour financer les enquêtes futures ?

Aux États-Unis, le Department of Justice a développé une expertise dans la saisie de cryptoactifs. Depuis 2021, le gouvernement américain a saisi plusieurs milliards de dollars en Bitcoin dans diverses affaires. Mais lorsque plusieurs États revendiquent une part des actifs, les négociations deviennent aussi intenses que dans un conflit territorial.

Cette dimension diplomatique de la finance criminelle numérique est l'une des grandes innovations de la décennie en matière de droit international. Elle oblige les États à créer de nouvelles normes, souvent en urgence et sous pression.

PARTIE V

Enjeux et Perspectives

Au-delàdesfaits,cetteaffaire soulève des questions qui dépassent largement le cas d'Anthony Coronadi. Elle interroge l'état du monde.

CHAPITRE 13

Le Crime a Adopté le Capitalisme Numérique

L'une desconclusions lesplus troublantes decetteaffaire est peut-être la plus simple : le crime organisé moderne ne ressemble plus à la mafia des films. Il ressemble à une startup.

Externalisation des tâches, décentralisation des opérations, recrutement horizontal via des plateformes numériques, paiements instantanés, logistique optimisée, service client. Le Dark Web a importé le playbook du capitalisme numérique pour le mettre au service de l'illégalité.

Cette mutation a des conséquences profondes :

- Elle rend le crime plus accessible — n'importe qui avec une connexion peut y entrer.
- Elle augmente l'échelle — un réseau peut opérer globalement sans jamais se réunir physiquement.
- Elle rend le démantèlement plus difficile — pas de chef unique, pas de QG, pas de frontières.
- Elle normalise le crime — emballé comme un service, il perd une partie de sa charge symbolique.

Le modèle Crime-as-a-Service (CaaS) est aujourd'hui une réalité documentée par les agences de cybersécurité mondiales. On peut louer un ransomware, sous-traiter une cyberattaque, acheter des données volées comme on achète une licence logicielle.

> Selon Europol, le marché mondial de la cybercriminalité dépasse désormais 8 000 milliards de dollars par an — soit plus que le PIB de nombreuses économies nationales.

CHAPITRE 14

Vers une Justice Transnationale ?

La grande frustrationque révèle cette affaireestl'inadéquation entre la vitesse du crime numérique et la lenteur des institutions judiciaires. Peut-on imaginer une justice à la hauteur du défi ?

Plusieurs pistes sont actuellement explorées à l'échelle internationale :

Traité international sur la cybercriminalité

La Convention de Budapest (2001) reste le seul instrument véritablement global. Un nouveau traité onusien est en négociation depuis 2019 mais se heurte aux divergences entre pays démocratiques et régimes autoritaires.

Tribunal international pour le cybercrime

L'idée circule dans les cercles académiques et diplomatiques. Elle se heurte aux questions de souveraineté : aucun État ne veut abandonner sa compétence judiciaire sur son territoire numérique.

Agences transnationales spécialisées

Europol a étendu son mandat au cybercrime. Des partenariats publics-privés émergent entre agences gouvernementales et entreprises de cybersécurité. Mais les moyens restent insuffisants.

Régulation des cryptoactifs

L'Union Européenne a adopté le règlement MiCA en 2023. D'autres juridictions suivent. L'encadrement financier reste cependant fragmenté et facilement contournable via des pays tiers.

CHAPITRE 15

Ce que Cette Affaire Change — ou Pas

Lesgrandesaffairesjudiciairesont parfois uneffetd'accélérateur sur les réformes institutionnelles. Parfois. L'affaire Coronadi sera-t-elle de celles-là ?

Ce qui a changé concrètement :

- Des intermédiaires ontété arrêtésdans trois pays.
- Des centaines de millions de dollars en crypto ont été saisis.
- La coopération judiciaire entre les trois pays concernés s'est renforcée.
- Des procédures d'analyse blockchain ont été partagées et améliorées.

Ce qui n'a pas changé :

- Le réseauce ntral —« Liston » — reste opérationnel ou a été remplacé.
- Les marchés du Dark Web continuent de fonctionner.
- L'absence de cadre juridique international unifié persiste.
- Les mules continuent d'être recrutées en masse via des annonces banales.
- La frontière numérique reste imperméable à la juridiction territoriale.

Anthony Coronadi a cru acheter un raccourci vers la performance physique. Il a servi de révélateur involontaire d'une réalité bien plus vaste : au XXIe siècle, un colis peut être local, mais le crime qu'il transporte est déjà mondial.

« La souveraineté judiciaire reste territoriale, alors que la criminalité numérique est transfrontalière par nature. »

Cette affaire ne clôt rien. Elle ouvre des questions que les États, les législateurs et les citoyens devront impérativement traiter dans les années qui viennent. Car le Dark Web, lui, n'attend pas.

PARTIE VI

Comprendre la Technologie

Pour aller au fond de l'affaire, il faut comprendre les outils. La technologie n'est pas neutre : elle structure les possibles et les impossibles de la criminalité numérique.

CHAPITRE 16

Comment Fonctionne le Réseau Tor

Torest la porte d'entrée du Dark Web. Comprendre son fonctionnement permet de saisir pourquoi il est si difficile à surveiller — et pourquoi il reste néanmoins vulnérable.

Le principe fondateur de Tor est le « routage en oignon ». Chaque paquet de données est enveloppé dans plusieurs couches de chiffrement, comme les couches d'un oignon. Il transite ensuite à travers au minimum trois nœuds de relais, chacun ne connaissant que le nœud précédent et le nœud suivant, jamais la source ni la destination finales.

Les trois nœuds du circuit Tor :

Nœud d'entrée (Guard Node)

Connaît l'adresse IP réelle de l'utilisateur mais pas sa destination. C'est le maillon le plus sensible du circuit.

Nœud intermédiaire (Middle Relay)

Ne connaît ni la source ni la destination. Simple relais qui fait transiter les données chiffrées.

Nœud de sortie (Exit Node)

Connaît la destination finale mais pas l'identité de l'utilisateur. Point le plus surveillé par les agences de renseignement.

La vulnérabilité principale de Tor réside dans ce qu'on appelle l'attaque de corrélation temporelle : si un adversaire contrôle à la fois le nœud d'entrée et le nœud de sortie, il peut théoriquement corréler les flux et identifier l'utilisateur. C'est l'une des techniques que les agences de renseignement comme la NSA explorent depuis des années.

Pour les marchés du Dark Web, la question n'est pas tant Tor lui-même que les comportements humains qui le court-circuitent : connexion à Tor depuis sa propre IP sans précaution, réutilisation d'identifiants, utilisation d'un même portefeuille crypto
pour des transactions légales et illégales.

En 2014, l'opération Onymous menée par Europol et le FBI a fermé plus de 400 sites .onion en exploitant des failles de configuration et non des vulnérabilités du protocole Tor lui-même.

CHAPITRE 17

La Forensique Numérique au Service de l'Enquête

L'investigationnumérique — ou forensique digitale — est la discipline qui permet aux enquêteurs d'extraire, préserver et analyser les preuves numériques. Dans l'affaire Coronadi, elle a joué un rôle central.

Les enquêteurs disposent aujourd'hui d'un arsenal d'outils spécialisés :

Analyse de métadonnées

Chaque fichier numérique contient des métadonnées : date de création, logiciel utilisé, coordonnées GPS pour les photos, adresse MAC de l'appareil. Ces informations, souvent ignorées par les suspects, constituent une mine d'indices pour les enquêteurs.

Traçage des transactions blockchain

Des sociétés comme Chainalysis ou Elliptic proposent des outils d'analyse blockchain utilisés par des dizaines d'agences gouvernementales. Ils permettent de cartographier les flux de cryptomonnaie et d'identifier les exchanges qui reçoivent les fonds illicites.

Infiltration des marchés

Des agents undercover créent des comptes sur les marchés du Dark Web, effectuent des achats, construisent une réputation de vendeur. Cette technique, encadrée juridiquement, a permis de nombreuses arrestations de haut niveau.

Corrélation de pseudonymes

Un même individu utilise souvent les mêmes habitudes sur différentes plateformes. La corrélation entre pseudonymes, horaires de connexion, styles d'écriture et patterns comportementaux permet parfois d'identifier des suspects que la technologie seule ne révèle pas.

CHAPITRE 18

La Sécurité Opérationnelle des Réseaux Criminels

Comment lesréseauxcriminels organisés maintiennent-ils leur sécurité face à des adversaires technologiquement sophistiqués ? La réponse tient en un concept : l'OPSEC, ou sécurité opérationnelle.

L'OPSEC criminelle s'articule autour de plusieurs principes fondamentaux :

- Cloisonnement strict : chaque acteur ne connaît que ce dont il a besoin pour sa mission.
- Identités multiples et jetables : les pseudonymes changent régulièrement.
- Communications chiffrées : PGP ou protocoles dédiés comme Signal ou Wire.
- Mélange des fonds : les cryptomonnaies passent par des mixeurs avant d'être utilisées.
- Règle de silence : aucune information personnelle ne circule sur les canaux opérationnels.
- Compartimentation géographique : les acteurs ne se rencontrent jamais physiquement.

Paradoxalement, ce sont souvent les manquements à ces règles — et non leur application — qui conduisent aux arrestations. Un message envoyé depuis une connexion non anonymisée, une livraison vers une adresse personnelle, un portefeuille crypto utilisé pour un achat légal identifiable. Les erreurs humaines restent la première faille des réseaux criminels numériques.

Dans l'affaire Coronadi, c'est précisément une erreur logistique — le choix d'une adresse de livraison traçable — qui a permis aux enquêteurs d'entrer dans le système. La sophistication technologique du réseau n'a pas résisté à la banalité d'un code postal.

PARTIE VII

Dimensions Sociétales

Lacriminaliténumériquen'estpas qu'un problème technique ou juridique. Elle révèle des fractures et des tensions au cœur de nos sociétés.

CHAPITRE 19

La Demande : Pourquoi les Consommateurs Entrent dans ce Monde

Onparle beaucoupdes fournisseurs, desréseaux, des trafiquants. On parle moins de la demande. Or sans demande, pas de marché. Comprendre pourquoi des millions d'individus font appel aux marchés du Dark Web est essentiel pour appréhender le phénomène dans sa globalité.

Les profils des acheteurs sur les marchés du Dark Web sont beaucoup plus variés qu'on ne l'imagine généralement :

Le consommateur de substances

Personne qui préfère la discrétion et la qualité contrôlée du Dark Web aux risques du marché de rue. Souvent pas un criminel au sens classique.

Le chercheur de performance

Comme Anthony — sportif, professionnel, qui cherche un avantage compétitif sans passer par les voies légales.

Le collectionneur d'armes

Dans les pays où la législation est restrictive, certains achètent des armes pour des raisons qu'ils considèrent légitimes.

L'acheteur de données

Entreprises ou individus qui achètent des bases de données personnelles volées pour diverses raisons, légales ou illégales.

Le consommateur de contenus interdits

La catégorie la plus grave, incluant des contenus dont l'existence même constitue un crime.

Cette diversité de profils complique les réponses politiques. Une approche punitive uniforme ne tient pas compte de la multiplicité des motivations et des degrés de nocivité sociale. Certains pays européens expérimentent des approches de réduction des risques pour les consommateurs de drogues, en reconnaissant que la criminalisation ne réduit pas la demande — elle la déplace.

CHAPITRE 20

Inégalités Numériques et Vulnérabilité au Recrutement

Lesmulespostales commeAmanda ne tombent pas dans le piège par hasard. Elles sont identifiées, ciblées, recrutées. Et les réseaux criminels savent exactement où les trouver.

Le recrutement des exécutants de bas niveau suit des patterns précis :

- Ciblage des personnes en difficulté financière via des forums d'emploi et des réseaux sociaux.
- Annonces formulées comme des opportunités légitimes de travail à domicile.
- Premier contact banal et rassurant, escalade progressive vers des tâches illicites.
- Paiements rapides qui créent une dépendance économique.
- Menaces et pression psychologique une fois la personne impliquée.

Ce modèle exploite systématiquement les inégalités sociales et économiques. Dans les pays à forte précarité, le recrutement est massif. Mais les pays riches ne sont pas épargnés : la montée des inégalités, la précarisation du travail, l'isolement social créent des poches de vulnérabilité que les réseaux criminels cartographient avec précision.

> Selon une étude du National Crime Agency britannique, la majorité des mules postales identifiées au Royaume-Uni entre 2020 et 2024 étaient des personnes sans emploi stable ayant répondu à des annonces sur des plateformes légitimes.

CHAPITRE 21

Protéger sa Trace Numérique : Ce que Chacun Peut Faire

Au-delàdes réponsesinstitutionnelles,il existe unedimension individuelle à la cybersécurité que cette affaire met en lumière. La naïveté numérique est une vulnérabilité collective.

Pour les utilisateurs ordinaires :

- Nejamaiscliquersurdesliens nonsollicités promettant des gains faciles.
- Vérifier systématiquement les vendeurs en ligne et les opportunités de travail.
- Comprendre que la cryptomonnaie n'est pas anonyme — elle est pseudonyme.
- Signaler tout colis ou demande de réexpédition suspecte aux autorités.
- Former les jeunes aux risques de la consommation sur le Dark Web.

Pour les entreprises et institutions :

- Investirda nslaformationà la cybersécurité à tous les niveaux.
- Coopérer activement avec les autorités en cas de suspicion de trafic.
- Surveiller les canaux de recrutement utilisés par les réseaux criminels.
- Implémenter des vérifications KYC (Know Your Customer) robustes.
- Partager les informations sur les nouvelles tactiques criminelles.

La lutte contre la criminalité numérique ne peut pas être uniquement l'affaire des États et des forces de l'ordre. Elle suppose une culture de la vigilance numérique qui reste encore largement à construire dans nos sociétés.

ANNEXES

Documents de Référence

Chronologie de l'affaire

J-0 —Anthony Coronadipassesa commande sur un marché du Dark Web.

J+7 —Lecolis est expédié depuis Coventry, Royaume-Uni.

J+14 —Interception douanière aux États-Unis. Ouverture d'une enquête fédérale.

J+30 —L'analyse blockchain révèle des centaines de transactions similaires.

J+45 —Identification d'Amanda comme point de réexpédition UK.

J+60 —Arrestation d'Amanda à Coventry. Saisie du matériel informatique.

J+90 —Lesflux financiers pointent vers l'Inde. Contact avec les autorités indiennes.

J+120 —Saisie de portefeuilles Bitcoin. Début de la coopération tripartite.

J+180 —Arrestation de plusieurs intermédiaires en Inde.

Aujourd'hui — « Liston » reste non identifié. L'enquête se poursuit.

Ressources et textes de référence

- Conventionde Budapestsur la cybercriminalité (2001) — Conseil de l'Europe
- EU Regulation MiCA (2023) — Régulation des marchés de cryptoactifs
- FATF Guidance on Virtual Assets (2019 & mises à jour) — Recommandations GAFI
- Europol Internet Organised Crime Threat Assessment (IOCTA) — Rapports annuels
- U.S. Department of Justice — Cryptocurrency Enforcement Framework (2020)
- UK National Crime Agency — Annual Threat Assessment
- Chainalysis Crypto Crime Report — Édition annuelle

CHAPITRE 22

Intelligence Artificielle et Cybercriminalité : la Prochaine Frontière

Cetteaffaire s'estdérouléedanslecontexte d'unetransformation technologique profonde : l'avènement de l'intelligence artificielle générative. Ses implications pour la cybercriminalité sont considérables.

Du côté des criminels, l'IA offre de nouvelles capacités :

- Génération defauxdocumentsd'identitéindétectables.
- Rédaction automatisée d'annonces de recrutement de mules ultra-ciblées.
- Création de deepfakes audio et vidéo pour des escroqueries à la confiance.
- Automatisation des attaques de phishing personnalisées à grande échelle.
- Optimisation des routes logistiques pour éviter les contrôles douaniers.

Du côté des enquêteurs, l'IA devient aussi un outil :

- Analyse automatisée demillionsdetransactions blockchain.
- Détection de patterns comportementaux sur les marchés du Dark Web.
- Corrélation de pseudonymes à travers des milliers de plateformes.
- Prévision des nouvelles routes de trafic avant leur activation.
- Traitement en temps réel des communications interceptées.

La prochaine génération de conflits entre la criminalité numérique et les forces de l'ordre sera largement algorithmmique. Des IA criminelles affronteront des IA judiciaires dans une course aux armements technologiques dont les enjeux humains sont immenses. L'affaire Coronadi, vue de ce prisme, n'est qu'un prélude.

NOTE DE L'AUTEUR

Sur les Choix Éditoriaux de cette Enquête

Cetebook est néd'un constat : lesaffairesde cybercriminalitésont régulièrement résumées en quelques paragraphes techniques qui en occultent la dimension humaine et politique. L'affaire Coronadi méritait un traitement plus approfondi.

J'ai choisi de partir du particulier — un homme, un colis, une erreur — pour aller vers le général : les structures du crime numérique mondial, les failles des systèmes judiciaires, les enjeux géopolitiques de la finance cryptée.

Certains détails ont été généralisés ou anonymisés pour protéger l'intégrité des enquêtes en cours. Les analyses et conclusions sont celles de l'auteur et n'engagent ni les autorités concernées ni les juridictions impliquées.

Ce que j'espère que vous retenez de cette lecture :

- La criminalité numérique n'est pas virtuelle — ses victimes sont bien réelles.
- L'anonymat technique ne protège pas des erreurs humaines.
- La coopération internationale est possible mais insuffisante.
- La réponse à ce défi est autant sociétale que technologique.
- Chaque clic, chaque transaction, chaque identité numérique laisse une trace.

Mohamed Ait Bellahcen Journaliste d'investigation numérique Mars 2026

SYNTHÈSE

Les Dix Leçons de l'Affaire Coronadi

Avant derefermerce dossier,voiciles dixenseignements que l'on peut tirer de cette enquête — dix vérités que cette affaire illustre avec une clarté troublante.

01. La banalité du crime numérique

La criminalité numérique n'est plus réservée aux hackers d'élite. Elle est accessible à tous — consommateurs comme exécutants — via des interfaces pensées pour le grand public.

02. La dissociation comme protection

Le cloisonnement des tâches est la principale défense des réseaux criminels. Il transforme chaque acteur en fusible ignorant l'ensemble du circuit.

03. La cryptomonnaie est un outil, pas une protection absolue

Le Bitcoin offre la pseudonymité, pas l'anonymat. L'analyse blockchain reste l'arme la plus efficace des enquêteurs financiers.

04. L'erreur humaine prime sur la faille technique

Dans la quasi-totalité des affaires résolues, c'est une erreur comportementale — pas une vulnérabilité technologique — qui a permis l'arrestation.

05. La géographie du crime est mondiale, celle de la justice reste locale

Cette inadéquation fondamentale est le principal avantage structurel dont bénéficient les réseaux criminels numériques.

06. Le Dark Web mimétise l'économie légale

En adoptant les codes du e-commerce, la criminalité numérique se normalise et s'industrialise simultanément.

07. La vulnérabilité sociale alimente le recrutement

Les mules, les intermédiaires, les exécutants de base sont majoritairement des personnes en situation de précarité économique.

08. L'IA va changer la donne des deux côtés

Les prochaines années verront une course aux armements algorithmiques entre criminalité numérique et forces de l'ordre.

09. La coopération internationale est nécessaire mais insuffisante

Elle existe, fonctionne partiellement, mais reste fragmentée, lente et soumise aux intérêts nationaux divergents.

10. La réponse est autant sociétale que technologique

Réduire la demande, éduquer au numérique, lutter contre la précarité : autant de leviers non-technologiques qui conditionnent l'efficacité de toute réponse institutionnelle.

L'Ère du Crime Fluide

Nousvivons à l'ère du crimefluide.Un crime qui n'a pas de siège social, pas de nationalité, pas de visage identifiable. Un crime qui recrute via LinkedIn, paye via Bitcoin, et livre via La Poste.

L'affaire que vous venez de lire n'est pas exceptionnelle. Elle est représentative. Chaque jour, des milliers de colis similaires circulent à travers le monde. Des milliers d'Amandas ouvrent et referment des cartons sans poser de questions. Des milliers d'Anthonys cliquent sur des sites qu'ils ne comprennent pas vraiment.

La vraie question n'est pas de savoir si nos systèmes judiciaires parviendront un jour à démanteler complètement ces réseaux. La vraie question est de savoir si nos sociétés sont prêtes à réfléchir honnêtement aux conditions qui les rendent possibles : la facilité de l'anonymat numérique, l'attrait de l'argent rapide, la déréglementation financière, et la lenteur collective à prendre la mesure du changement.

Mohamed Ait Bellahcen — Mars 2026

GLOSSAIRE

Dark Web
Partie d'Internet accessible uniquement via des logiciels spéciaux comme Tor. Non indexé par les moteurs de recherche classiques.

Tor (The Onion Router)
Logicielanonymisant qui fait transiter les données via plusieurs serveurs cryptés, masquant l'identité de l'utilisateur.

Bitcoin
Cryptomonnaie décentralisée créée en 2009. Transactions enregistrées sur une blockchain publique mais pseudonymes.

Monero
Cryptomonnaie à confidentialité renforcée. Les transactions sont privées et quasi-impossibles à tracer.

Blockchain
Registredistribué et immuable enregistrant toutes les transactions d'une cryptomonnaie. Outil central de l'analyse forensique financière.

Mule postale
Personne recrutée pour réceptionner et réexpédier des colis illicites, souvent sans en connaître le contenu exact.

PGP (Pretty Good Privacy)
Protocole de chiffrementutilisé pour sécuriser les communications électroniques. Standard sur le Dark Web.

Escrow
Dépôtde garantie numérique sur les marchés du Dark Web. Protège acheteurs et vendeurs jusqu'à confirmation de la transaction.

Crime-as-a-Service (CaaS)
Modèlecrimineloù des outils et services illicites sont loués ou vendus à d'autres criminels, comme des logiciels SaaS.

Analyse blockchain
Techniqueforensique permettant de retracer les flux de cryptomonnaie d'adresse en adresse pour identifier des suspects.

Fanzone

L'ODJ Media lance son premier fanzine et appelle les jeunes créateurs à participer

Dans un univers médiatique souvent formaté, L'ODJ Media ouvre un nouvel espace d'expression en lançant son premier fanzine, une publication indépendante dédiée à la créativité libre et aux talents émergents.

Contraction des mots fan et magazine, le fanzine est une revue artisanale et indépendante, historiquement associée aux cultures alternatives et aux passions créatives. Autoédité, souvent produit en petites séries, il repose sur un esprit DIY (Do It Yourself) où les créateurs gèrent eux-mêmes l'ensemble du processus : écriture, illustration, mise en page et diffusion.

Avec ce projet, L'ODJ Media souhaite offrir une tribune ouverte aux jeunes voix qui souhaitent s'exprimer autrement, en dehors des formats éditoriaux classiques. L'objectif : créer un espace d'expérimentation artistique et intellectuelle où l'imagination, l'engagement et la spontanéité priment.

Le fanzine accueillera une grande diversité de contributions : textes courts, poésie, chroniques, bande dessinée, illustrations, photographie, collages, réflexions sociales ou récits personnels. Aucun format rigide n'est imposé. La seule règle : l'authenticité et la créativité.

Fidèle à l'esprit originel des fanzines, cette publication sera produite en tirage limité, dans une logique non commerciale, accessible et collaborative. Plus qu'un simple support, il s'agit d'un laboratoire d'idées et de talents, où chaque contribution participe à construire une œuvre collective.

Illustrateurs, écrivains en herbe, étudiants, photographes, graphistes ou passionnés de culture : toutes les sensibilités créatives sont les bienvenues.

Dans un monde où les contenus sont souvent standardisés, le fanzine se veut un rappel simple mais essentiel : les grandes idées commencent parfois sur une simple page blanche.

Les jeunes créateurs intéressés peuvent dès maintenant proposer leurs contributions pour participer à ce premier numéro du fanzine L'ODJ, une aventure éditoriale qui ambitionne de révéler de nouvelles voix et de célébrer la liberté de création.itées dans cet ouvrage.

Contact : lodjmaroc@gmail.com