Roman LATTE

Coordinateur des Opérations Criminalistiques Cyber (COCRIM Cyber) : Un maillon clé pour la gestion des scènes de crimes cyber

Université BORDEAUX MONTAIGNE
Cyber criminalités

Promotion 2024-2025

Face à l'escalade et à la complexité croissante de la cybercriminalité, la gestion des scènes de crimes numériques est devenue un défi majeur pour les forces de l'ordre. Cet article propose l'instauration d'un rôle de "Coordinateur des opérations criminalistiques Cyber" au sein de la Gendarmerie Nationale française. Positionné stratégiquement au niveau régional, ce coordinateur serait un catalyseur essentiel pour optimiser la coordination, la fluidité et l'efficacité des enquêtes numériques complexes. Nous explorerons la nécessité de ce rôle, ses missions clés, le profil requis, ainsi que les avantages significatifs et les défis potentiels de son intégration dans le dispositif existant, en soulignant que ses bénéfices l'emportent largement sur les coûts d'implémentation pour renforcer la compétitivité de la Gendarmerie face aux cybercriminels.

Mots-clés :

Cybercriminalité

Gendarmerie Nationale

Criminalistique numérique

Scène de crime cyber

Coordination d'enquête

NTECH

C3N

Cyberdéfense

1. Introduction

L'ère numérique a profondément remodelé le paysage de la criminalité, engendrant une explosion de la cybercriminalité en termes de fréquence, de portée et de sophistication. Chaque année, les observations des agences nationales et internationales, notamment l'ANSSI, confirment dans leurs rapports, une hausse significative des incidents en 2024 de 15 % par rapport à l'année précédente, avec une prévalence alarmante de 30 % des rançongiciels et des attaques par compromission des chaînes d'approvisionnement, causant des préjudices économiques se chiffrant en milliards d'euros à l'échelle mondiale et nationale. Selon l'ANSSI, le coût global des cyberattaques en France s'élevait à 2 milliards d'euros en 2022. Les attaques ne se limitent plus à des intrusions isolées, mais se manifestent de plus en plus sous forme d'opérations complexes, ciblées et coordonnées, capables de paralyser des infrastructures vitales, de compromettre des données sensibles et d'engendrer des préjudices économiques et sociaux considérables. Des secteurs aussi cruciaux que la santé, l'administration publique, ou l'industrie sont désormais des cibles privilégiées, soulignant l'impérieuse nécessité pour les forces de l'ordre d'adapter leurs capacités d'investigation. La nature souvent transfrontalière et l'anonymat relatif des cybercriminels, conjugués à la volatilité extrême des preuves numériques, ajoutent une couche de complexité sans précédent aux enquêtes judiciaires.

En France, la Gendarmerie Nationale, par le biais de ses unités spécialisées et de sa compétence territoriale étendue, a développé une expertise reconnue dans la lutte contre la cybercriminalité. Cependant, la gestion des scènes de crimes numériques est intrinsèquement complexe. Elle requiert non seulement une expertise technique pointue pour l'acquisition forensique de données et la préservation de la chaîne de garde numérique, mais aussi une coordination stratégique agile entre des acteurs multiples, allant des DTNum (Diplôme Technique Numérique, ex-NTECH) sur le terrain aux instances d'investigation nationales comme le C3N (Centre de Lutte contre les Criminalités Numériques). La problématique actuelle réside précisément dans le défi de maintenir une cohérence et une efficacité maximales face à des attaques transversales et évolutives. Des lacunes dans la coordination peuvent entraîner des délais préjudiciables, une dispersion des expertises et une exploitation sous-optimale des preuves numériques, compromettant ainsi la robustesse et la célérité des procédures judiciaires.

Cet article propose d'analyser la pertinence et la nécessité d'un rôle central de "Coordinateur des opérations criminalistiques Cyber" au sein de la Gendarmerie. Nous démontrerons que ce maillon clé, doté d'une formation opérationnelle ancrée dans la réalité du terrain et d'une vision prospective, est indispensable pour structurer et fluidifier les enquêtes numériques complexes, combler un éventuel fossé entre les unités techniques de terrain et les instances d'investigation nationales, et, in fine, renforcer significativement la capacité de la Gendarmerie à assurer une coordination efficace et fluide entre les différents acteurs pour répondre à une cybercriminalité de plus en plus complexe. Pour ce faire, nous commencerons par une revue détaillée du paysage actuel de la cybercriminalité et une présentation approfondie du dispositif Gendarmerie en France.

Nous exposerons ensuite en détail les missions clés et le profil requis pour ce rôle stratégique. Enfin, nous analyserons les avantages substantiels et les défis potentiels liés à son implémentation, en soulignant que ses bénéfices l'emportent largement sur les coûts, et ce, dans l'optique de renforcer la capacité nationale à faire face à une menace cyber en constante évolution

2. Le paysage actuel de la cybercriminalité et le dispositif Gendarmerie en France

La lutte contre la cybercriminalité en France repose sur un maillage de compétences au sein de la Le Paysage Actuel de la Cybercriminalité et le Dispositif Gendarmerie en France

La lutte contre la cybercriminalité en France repose sur un maillage de compétences au sein de la Gendarmerie Nationale, structuré pour assurer une couverture territoriale et une expertise technique. Le premier échelon d'intervention est constitué par les DTNum (Fusionnement de deux services gendarmerie constitués des NTECH, enquêteurs nouvelle technologie et les SIC, les spécialistes des systèmes d'informations et de communication). Ces techniciens spécialisés, répartis sur l'ensemble du territoire, sont les primo-intervenants essentiels sur les scènes de crimes numériques locales. Leur mission est cruciale est de réaliser les premières constatations, assurer la préservation méthodique des preuves numériques, souvent éphémères, et exécuter les actes techniques initiaux indispensables à toute enquête. Ils peuvent être aidés localement dans les unités de terrain par des C'NTECH (Correspondant de Nouvelles Technologies) au niveau brigade. Au-dessus de cette strate opérationnelle, le C3N (Centre de Lutte contre les Criminalités Numériques), rattaché à l'Unité Nationale Cyber de la Gendarmerie Nationale (UNCyber), incarne le centre névralgique de l'expertise de haut niveau dans le domaine Cyber. Il assure une coordination nationale des enquêtes les plus complexes, apporte un soutien analytique approfondi et maintient une veille technologique stratégique indispensable pour comprendre et anticiper l'évolution des menaces.

Les limites d'un dispositif face à la complexité cybercriminelle

Si cette architecture permet une couverture territoriale indéniable et une capacité d'expertise reconnue, les attaques cybercriminelles modernes posent des défis qui peuvent mettre à l'épreuve son efficacité optimale. La nature de la cybercriminalité a profondément évolué : elle est désormais souvent transnationale, polymorphe et caractérisée par une rapidité d'exécution qui dépasse les schémas d'enquête traditionnels. Une attaque ciblée et multi-facettes peut, par exemple, impacter simultanément plusieurs entités géographiques et sectorielles, rendant obsolète une approche cloisonnée.

Cette complexité nouvelle exige une vision d'ensemble immédiate et une coordination agile qui ne sont pas toujours naturellement intégrées au niveau de chaque DTNum, dont le champ d'action reste intrinsèquement local. De même, le C3N, malgré son rôle national et stratégique, et les antennes C3N, au niveau régional, ne sont pas conçus pour une coordination opérationnelle minute par minute de chaque enquête complexe décentralisée ; leur rôle est plus axé sur l'expertise et la direction des affaires majeures. Il en résulte un risque de dispersion des efforts, de perte de cohérence dans la collecte des preuves et de rallongement des délais d'intervention, autant de facteurs critiques face à des cybercriminels qui exploitent la moindre faille organisationnelle.

Exemple de scène de crime Cyber, un scénario fictif révélateur des enjeux actuels

Imaginons un scénario, malheureusement de plus en plus réaliste : une cyberattaque d'envergure frappe simultanément plusieurs acteurs clés de la région bordelaise. Un groupe de hackers s'introduit par une "porte numérique" laissée ouverte dans le système informatique d'un hôpital, exigeant une rançon pour la restitution de données vitales de patients, mettant directement en péril la vie humaine. Simultanément, ces mêmes assaillants ciblent des fichiers décentralisés de la Direction Générale de la Sécurité Intérieure (DGSI) à Bordeaux pour obtenir des informations sensibles, menaçant la sécurité nationale. Dans le même laps de temps, un industriel local commercialisant des produits alimentaires pour les écoles de la périphérie de Bordeaux est également victime d'une intrusion, visant à paralyser sa chaîne de production, avec des conséquences économiques et sanitaires potentielles majeures. Une telle situation implique l'intervention urgente et coordonnée de multiples spécialistes Gendarmerie, potentiellement issus de différentes unités territoriales, face à des victimes aux enjeux distincts mais potentiellement liés par un même mode opératoire, une même infrastructure d'attaque et une même origine. C'est précisément dans ce type de scénario, où la complexité, la transversalité et la gravité des impacts sont extrêmes, qu'un maillon de coordination dédié et agile s'avère absolument indispensable pour une gestion efficace, harmonisée et réactive de la scène de crime numérique, permettant de maximiser les chances d'identification des auteurs et de minimiser les préjudices.

3. <u>Le coordinateur des opérations criminalistiques cyber : un maillon stratégique</u>

Le Coordinateur des opérations criminalistiques Cyber est la réponse structurelle et fonctionnelle à un besoin pressant d'orchestration et de centralisation dans la gestion des enquêtes numériques complexes. Ce rôle, envisagé comme une fonction pivot au niveau régional, serait le pilier assurant la cohérence, la fluidité et l'efficacité des actions menées sur le terrain, transformant des interventions potentiellement isolées en une stratégie d'investigation unifiée et puissante.
Ses missions clés incluraient :

- **Supervision stratégique des opérations complexes cyber** :
  Au-delà de la simple supervision administrative, le coordinateur serait le véritable architecte de la réponse opérationnelle sur les affaires les plus sensibles et multidimensionnelles. Reprenons l'exemple de l'attaque de Bordeaux touchant simultanément un hôpital, la DGSI et un industriel. Sans coordination centrale, ces incidents pourraient être traités comme des affaires distinctes, menant à des efforts redondants, des pertes d'information ou des stratégies d'investigations divergentes. Le coordinateur chapeauterait l'ensemble de ces investigations, assurant une vision d'ensemble agrégée et dynamique. Il serait chargé d'identifier les liens entre les différentes intrusions (même mode opératoire, même groupe d'acteurs, même source initiale), d'harmoniser les protocoles de recueil de preuve, de centraliser les informations cruciales et d'allouer les ressources (humaines et techniques) de manière optimale sur les différents fronts. Sa capacité à prioriser les actions en fonction des enjeux (sauvegarde de vies, protection de données sensibles, continuité d'activité économique) et à maintenir une communication constante entre les équipes DTNum dispersées serait primordiale pour éviter le "chaos" inhérent aux scènes de crimes numériques étendues.

- **Interface technique et stratégique avec le directeur d'enquête et le magistrat** :
  C'est une mission fondamentale qui positionne le coordinateur comme un traducteur et un conseiller privilégié de l'autorité judiciaire. Le monde cyber est intrinsèquement technique et évolue rapidement, rendant difficile pour les non-spécialistes, y compris les magistrats et directeurs d'enquête, d'appréhender pleinement la portée et les implications des preuves numériques. Le coordinateur aurait pour rôle de démystifier la complexité technique, en vulgarisant les concepts (par exemple, expliquer le fonctionnement d'un ransomware, la traçabilité d'un portefeuille de cryptomonnaies ou la nature des logs informatiques) et en traduisant les découvertes techniques en éléments intelligibles et actionnables d'un point de vue judiciaire. Il conseillerait sur les orientations stratégiques à prendre (ex: opportunité d'une perquisition, utilisation de techniques d'investigation spécifiques, délais de réponse critiques), sur les implications légales des choix techniques, et sur les contraintes et les opportunités offertes par l'environnement numérique. Cette interface garantit que les décisions judiciaires sont éclairées par une compréhension technique solide, et que les actions techniques sont menées dans le respect du cadre légal.

- **Liaison et mobilisation des experts** :
  La cybercriminalité ne se résout pas toujours avec les seules ressources internes. Le coordinateur agirait comme un hub d'expertise. Il aurait la responsabilité d'identifier et de mobiliser les expertises nécessaires au moment opportun, qu'elles soient internes à la Gendarmerie (comme des spécialistes du C3N pour des analyses complexes, des experts en cryptographie ou en ingénierie inverse de malwares), ou externes (agences nationales comme l'ANSSI, partenaires privés spécialisés en cybersécurité, ou des universitaires pour des recherches spécifiques). Il faciliterait les échanges d'informations sécurisés, s'assurerait que les besoins des enquêteurs sont clairement formulés aux experts, et que les retours des experts sont correctement intégrés dans la stratégie d'enquête. Cette capacité à sourcer et à intégrer des savoir-faire multiples et complémentaires est un atout majeur pour faire face à la diversité des menaces.

- **Analyse prospective et veille stratégique** :
  Au-delà de la gestion réactive des enquêtes en cours, une dimension cruciale du rôle du coordinateur est sa vision proactive. Il ne se contenterait pas de traiter le passé ou le présent ; il s'engagerait dans une veille permanente sur les nouvelles techniques d'attaques cybercriminelles, les vulnérabilités émergentes, l'évolution des outils utilisés par les criminels (ex: l'usage de l'intelligence artificielle par les attaquants), et les tendances géopolitiques qui influencent la cybermenace. Cette veille lui permettrait d'anticiper les menaces futures, d'adapter les stratégies d'investigation en amont, de proposer des évolutions de doctrines opérationnelles, et d'aider à la formation quasi quotidienne pour les Dtnum de son secteur. Il serait ainsi un acteur clé de l'adaptation continue de la Gendarmerie face à un adversaire en constante mutation.

4. **Compétences et profil du coordinateur : l'opérationnel avant le bureaucrate**

Le succès et la légitimité du rôle de Coordinateur des opérations criminalistiques Cyber reposent intrinsèquement sur la sélection rigoureuse et la formation continue d'individus aux compétences multidimensionnelles, capables de naviguer avec aisance entre les impératifs techniques, stratégiques et judiciaires. Il est impératif que ce coordinateur ne soit en aucun cas perçu ou ne devienne un simple maillon bureaucratique ou un conseiller technique déconnecté des réalités opérationnelles du terrain. Sa valeur ajoutée réside précisément dans sa capacité à rester profondément opérationnel et pragmatique.
Son profil idéal et les compétences qu'il doit incarner peuvent être décomposés comme suit :

- **Une expertise technique cyber de pointe et constamment actualisée** :
  Le coordinateur doit posséder une connaissance exhaustive et pratique des technologies d'information et de communication, des architectures réseau, des systèmes d'exploitation, et des méthodologies d'attaques cybercriminelles (ransomwares, phishing avancé, APT, etc.). Cette expertise doit inclure une maîtrise approfondie de la forensique numérique (acquisition, analyse, préservation des preuves), des techniques d'analyse de malwares, et des outils d'investigation spécifiques. Plus encore, cette connaissance doit être dynamique et au jour le jour. Le monde cyber évolue à une vitesse exponentielle; sans une veille technologique constante, une participation active à des exercices de crise et à des formations pratiques non déconnectées du terrain, l'expertise du coordinateur perdrait rapidement de sa pertinence. Il doit être capable de comprendre les DTNum, de parler leur langage, et d'évaluer la faisabilité et la pertinence de leurs actions techniques.

- **Maîtrise approfondie du cadre juridique et judiciaire** :
  Au-delà de la technique, le coordinateur doit posséder une connaissance solide du droit pénal applicable à la cybercriminalité (infractions, procédures, chaîne de garde numérique, règles de preuve).

- Il doit comprendre les impératifs des magistrats et des directeurs d'enquête, savoir traduire les éléments techniques en langage juridique clair et concis, et conseiller sur les meilleures approches pour garantir la légalité et la recevabilité des preuves devant les tribunaux. Cette double compétence technique et juridique est essentielle pour faire le lien entre le "comment" (technique) et le "pourquoi" (judiciaire).

- **Compétences managériales, de leadership et interpersonnelles affirmées** :
  Le rôle de coordinateur est avant tout un rôle de chef d'orchestre. Il doit être capable de :
  - Diriger et motiver des équipes multidisciplinaires, souvent sous forte pression.
  - Communiquer de manière claire, concise et adaptée à des interlocuteurs variés (techniciens, enquêteurs, magistrats, experts externes, victimes).
  - Négocier et arbitrer en cas de divergences techniques ou stratégiques.
  - Gérer des projets complexes, en définissant des objectifs, des plannings, et en allouant des ressources.
  - Faire preuve de résilience et de sang-froid face à des situations de crise et des découvertes sensibles. Ces compétences sont cruciales pour assurer une fluidité dans les échanges et une coordination efficace.

- **Esprit d'analyse, de synthèse et d'anticipation** :
  Le coordinateur doit avoir une capacité exceptionnelle à synthétiser des volumes massifs d'informations techniques, tactiques et stratégiques. Il doit pouvoir identifier des schémas d'attaques émergents, corréler des éléments qui, à première vue, ne semblent pas liés, et dégager des pistes d'enquête pertinentes. Sa vision prospective est également primordiale : anticiper les évolutions des menaces et des outils des cybercriminels, afin d'adapter les stratégies d'investigation et de proposer des évolutions capacitaires pour la Gendarmerie.

- **Positionnement Stratégique** :
  Son placement "au-dessus des DTNum Gendarmerie mais en dessous du C3N UNCyber et des antennes C3N" n'est pas qu'une question de hiérarchie administrative; c'est une architecture fonctionnelle pensée pour l'efficacité. Ce positionnement permet au coordinateur d'avoir une vision régionale globale des cybermenaces, de structurer les enquêtes complexes menées au niveau local par les DTNum (en leur apportant un soutien tactique et stratégique) et d'assurer une remontée d'information qualifiée, synthétisée et pertinente vers le C3N, tout en bénéficiant de son expertise de pointe et de sa vision nationale. Ce rôle est conçu pour combler un "vide" opérationnel, transformant une série d'interventions locales potentielles en une stratégie d'enquête coordonnée et puissante.

5. Avantages et défis de l'intégration d'un coordinateur cyber

L'intégration d'un Coordinateur des opérations criminalistiques Cyber au sein de la Gendarmerie Nationale française promet des bénéfices substantiels, essentiels à la modernisation de sa réponse face à la cybercriminalité grandissante.

5.1. Avantages opérationnels et stratégiques

- **Efficacité et réactivité accrues des enquêtes :**
  La centralisation de la coordination permettrait une orchestration plus fluide des enquêtes complexes. Plutôt que de multiples enquêtes fragmentées, le coordinateur garantirait une vision d'ensemble, permettant un engagement des ressources (humaines et techniques) plus judicieuse, une priorisation des actions et une synergie accrue entre les équipes Cyber DTNum. Cela se traduirait par des délais d'investigation réduits et une capacité de réaction plus rapide face à l'évolution des menaces en temps réel.

- **Vision globale et cohérence opérationnelle :**
  Dans des scénarios complexes comme l'attaque de Bordeaux, où plusieurs entités sont touchées simultanément, le coordinateur serait le garant d'une compréhension unifiée de l'incident. Il permettrait de corréler des éléments qui, à première vue, pourraient sembler disparates, d'identifier des modes opératoires communs et de relier des attaques apparemment distinctes pour révéler des campagnes cybercriminelles organisées, assurant ainsi une stratégie d'investigation cohérente et maximisant les chances d'identifier et de neutraliser les auteurs.

- **Optimisation des procédures judiciaires et qualité de la preuve :**
  Le rôle d'interface du coordinateur entre le monde technique et le monde judiciaire est fondamental. Il serait en mesure de "traduire" la complexité des découvertes techniques en langage juridique clair pour les magistrats et directeurs d'enquête. Cette facilitation des échanges garantirait une meilleure compréhension des enjeux, une conformité rigoureuse aux exigences légales (notamment concernant la chaîne de garde numérique), et in fine, une robustesse accrue des preuves présentées devant les tribunaux, améliorant la probabilité de condamnations et de démantèlement des réseaux cybercriminels.

- **Meilleure gestion des ressources et capitalisation des connaissances :**
  En identifiant précisément les besoins en expertise et en matériel sur les différentes scènes de crimes, le coordinateur optimiserait l'allocation des compétences et des moyens disponibles. Il jouerait également un rôle clé dans la capitalisation des retours d'expérience, permettant à la Gendarmerie d'affiner continuellement ses protocoles d'investigation, ses méthodes de formation et ses outils, renforçant ainsi ses capacités à long terme.

- **Renforcement de la compétitivité stratégique :**
  En assurant une veille technologique et une analyse prospective des tendances de la cybercriminalité, le coordinateur permettrait à la Gendarmerie de rester à la pointe des techniques d'investigation. Cette capacité d'anticipation est cruciale pour ne pas être dépassé par l'ingéniosité des cybercriminels, assurant ainsi une protection plus efficace de la population, des infrastructures critiques et de la souveraineté numérique du pays.

5.2. Défis et enjeux

L'intégration d'un tel rôle, bien que nécessaire, soulève des défis significatifs qui devront être anticipés et gérés avec une stratégie robuste :

- **Coût budgétaire initial et entretien de l'expertise :**
  La création de postes de coordinateurs requiert un investissement financier non négligeable. Cela inclut non seulement les salaires de profils hautement qualifiés, mais aussi les coûts liés à leur formation initiale extrêmement poussée et, surtout, à leur formation continue. Le maintien à niveau des compétences techniques et juridiques dans un domaine en perpétuelle mutation exige des budgets récurrents pour l'accès à des outils spécialisés, des certifications avancées et des plateformes de veille. Cet aspect financier peut constituer un frein majeur à une adoption rapide et généralisée.

- **Complexité de l'intégration et risque de chevauchement des compétences :**
  L'introduction d'un nouveau maillon dans une structure organisationnelle existante et bien définie (DTNum, C3N, Sections de Recherches) impose une délimitation extrêmement précise des rôles et des responsabilités. Sans une charte claire et une communication transparente, il existe un risque avéré de chevauchement de compétences, de conflits d'autorité ou de perception d'une "couche" hiérarchique superflue. Cela pourrait entraîner des frictions internes, une dilution des responsabilités et, paradoxalement, un ralentissement des processus d'enquête plutôt qu'une optimisation. La réussite de l'intégration dépendra de l'adhésion de l'ensemble des acteurs.

- **Résistance au changement et acceptation organisationnelle :**
  Tout changement structurel majeur peut générer une résistance naturelle. Les personnels DTNum pourraient craindre une perte d'autonomie ou de reconnaissance de leur expertise locale, tandis que le C3N, ou antenne C3N, niveau régionale, pourraient percevoir une remise en question de certaines de ses prérogatives de coordination nationale. Vaincre cette inertie et favoriser une culture de collaboration nécessitera une communication interne intensive, des démonstrations concrètes de la valeur ajoutée du coordinateur et une implication des acteurs existants dans la définition et l'évolution du rôle.

- **Dépendance vis-à-vis d'une expertise rare et spécifique :**
  Le profil recherché pour ce coordinateur est celui d'un expert polyvalent (technique, juridique, managérial) et opérationnel. Ces profils sont rares et très demandés, tant dans le secteur public que privé. Une concentration de cette expertise sur un nombre limité de coordinateurs pourrait créer un point de vulnérabilité. En cas d'absence, de départ ou si la charge de travail dépasse la capacité d'un coordinateur, l'efficacité de la coordination régionale pourrait être compromise. Il sera crucial d'anticiper la pérennisation de cette expertise par des plans de carrière, de formation continue, et des mécanismes de relève ou de mutualisation.

- **Charge de travail potentiellement écrasante et risque de surcharge :**
  Si le rôle de coordinateur s'avère aussi efficace et indispensable que prévu, il est probable que la demande pour ses services augmente rapidement. Une charge de travail trop importante, en l'absence d'un nombre suffisant de coordinateurs ou de mécanismes de soutien, pourrait conduire à une surcharge, une diminution de la qualité de la coordination, voire un épuisement professionnel des individus occupant ces postes. Une planification des effectifs en fonction de l'évolution de la menace est donc primordiale.

6. Conclusion

L'émergence d'un **"Coordinateur des opérations criminalistiques Cyber"** au sein de la Gendarmerie Nationale française n'apparaît pas seulement comme une proposition pertinente, mais comme une **nécessité impérieuse** face à l'évolution constante et rapide du paysage de la cybercriminalité. Ce rôle, stratégiquement positionné au niveau régional, est **le maillon clé manquant** pour combler le fossé actuel entre l'expertise technique de terrain, souvent fragmentée, et une vision stratégique nationale cohérente et unifiée.

Optimisation de la gestion des scènes de crimes numériques

La capacité de ce coordinateur à **superviser, coordonner et anticiper** les opérations est primordiale. Il servirait d'**interface cruciale** avec l'autorité judiciaire, facilitant la prise de décision rapide et éclairée, essentielle face à la volatilité des preuves numériques. Une telle centralisation permettrait une **gestion optimisée des scènes de crimes numériques complexes**, garantissant la collecte exhaustive et l'analyse efficiente des éléments, souvent disséminés et éphémères. Cela se traduirait par une réduction significative des délais d'enquête et une amélioration de la qualité des preuves présentées devant les tribunaux, augmentant ainsi les chances de succès des poursuites judiciaires.

Une vision stratégique et une meilleure anticipation

Bien que son implémentation puisse engendrer des défis en termes de coût initial, de formation spécialisée et d'intégration dans les structures existantes, il est manifeste que les bénéfices en matière d'**efficacité opérationnelle**, de **vision globale** et de **renforcement de la capacité d'anticipation** l'emportent très largement. Le Coordinateur des opérations criminalistiques Cyber ne serait pas qu'un gestionnaire, mais aussi un **acteur clé de la veille stratégique**, capable d'identifier les nouvelles tendances d'attaques, d'adapter les protocoles d'intervention et de diffuser les bonnes pratiques au sein des unités. Cette capacité proactive est indispensable pour contrer des cybercriminels de plus en plus organisés et innovants.

Un impératif pour la souveraineté numérique de la France

En investissant résolument dans ce rôle, la Gendarmerie Nationale renforcerait de manière significative sa posture dans un domaine où elle doit absolument **rester compétitive face aux cybercriminels**. C'est un engagement fort envers la **protection de la population**, des **infrastructures critiques** et, plus largement, de la **souveraineté numérique de la France** face à une menace omniprésente et en constante mutation. Le Coordinateur des opérations criminalistiques Cyber n'est pas un luxe, mais un **impératif stratégique majeur** pour l'avenir de la lutte contre la cybercriminalité en France, posant les bases d'une réponse plus résiliente et agile face aux défis numériques de demain.

7. Références bibliographiques

→ Rapports annuels de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) concernant les panoramas de la Cybermenace 2023 - 2024

→ Note express Gendarmerie n° 28579 – 09 JUILLET 2020 relative à la formation des enquêteurs technologies numériques (LP NTECH).

→ CIRCULAIRE n ° 61 00 0 /D GGN /C EGN /D C /B F C SE d u 29 j u i n 2 02 3 relative à la sélection et à la formation des COordinateurs des opérations de Criminalistique de la Gendarmerie Nationale (COCrim).

→ CIRCULAIRE n° 16000 – 23 FEV 2008 DEF/GEND/OE/SDPJ/PJ relative à la lutte contre la délinquance liée aux technologies numériques.

→ CIRCULAIRE n ° 1 83 00 0 /GEN D /D OE/ SD PJ /B PJ du 24 décembre 2012 relative à l'emploi du coordinateur des opérations de criminalistique

→ Diplôme Technique Cyber-Numérique paru au journal officiel avec l'arrêté du 10 mars 2025 fixant les conditions de délivrance du diplôme technique cyber-numérique.

→ Discussion et échange avec l'adjudant FERNANDES Alexandre affecté à la section opérationnelle de lutte contre les cybermenaces à Bordeaux.