MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

PLAN CYBER DE LA POLICE NATIONALE

2022-2027

POLICE
NATIONALE

La cybercriminalité :

Une menace globale

L'ensemble de la société est aujourd'hui menacée par la cybercriminalité : menace contre l'État et les institutions publiques lorsqu'elle affecte les intérêts fondamentaux de la nation, menace contre le système économique lorsque les réseaux criminels s'attaquent aux systèmes d'information des entreprises et menace contre les citoyens lorsqu'elle s'immisce dans leurs usages digitaux quotidiens.

Une menace protéiforme

Si les cibles des cybercriminels sont plurielles, la nature des menaces est aussi très variée : la cybercriminalité englobe les atteintes directes aux technologies alors objets de l'infraction mais également l'utilisation par les criminels des systèmes d'information et des réseaux de communication, dont les réseaux chiffrés, comme support ou moyen de commettre une infraction.

Une menace en pleine expansion

Dans notre société hyper-connectée, l'usage quotidien d'Internet et de ses outils numériques représente aussi une opportunité pour les délinquants et impose aux services d'enquête de renouveler en permanence leur stratégie et le traitement de ces nouvelles formes d'infractions. Au-delà de la lutte contre les cyberattaques qui portent atteinte aux intérêts fondamentaux de l'État, nous sommes confrontés à une véritable cybercriminalité de masse à laquelle il faut sans cesse s'adapter. Désormais, chaque procédure peut avoir un volet numérique, que les enquêteurs doivent être en capacité de développer.

C'est pour répondre à ces enjeux à la fois qualitatifs (des infractions variées et de plus en plus complexes) et quantitatifs (les outils numériques et les réseaux de communication utilisés pour la délinquance de masse comme pour l'activité des organisations criminelles) que la police nationale renouvelle son dispositif de lutte contre la cybercriminalité à travers la mise en œuvre d'un ambitieux plan d'action quinquennal.

Panorama des principales menaces cyber

La technologie, comme objet de l'infraction

1. Les atteintes aux systèmes de traitement automatisé de données (STAD) :

- ***les rançongiciels*** (ou ransomware) : chiffrement des données d'un ordinateur ou d'un serveur informatique. Pour les recouvrer, la victime doit payer une rançon en monnaie virtuelle (bitcoin le plus souvent). Certains rançongiciels exfiltrent également les données de leurs victimes et les attaquants peuvent alors extorquer ces dernières en menaçant de divulguer les informations captées.

Les niveaux des rançons exigées augmentent, la fréquence des attaques s'est accrue, les victimes ciblées sont de plus en plus sensibles.

- ***les attaques en déni de service distribuées*** (DDOS) : rendre indisponibles des systèmes d'information pour des motifs de subversion ou d'ingérence étrangère.

Exemples récents :

1. *Le système informatique de l'ANTAI a été bloqué le 15 septembre 2020 par un grand nombre de connexions simultanées.*
2. *Le Centre National d'Enseignement à Distance (CNED) a vu son site Internet perturbé les 6 et 8 avril 2021 à la suite de flux importants en provenance de Thaïlande, Russie, Chine et des Philippines.*

2. Les atteintes aux systèmes de paiement :

- ***le phishing*** : vol des données de carte bancaires sur Internet.
- ***les troyens bancaires :*** virus captant en ligne les données bancaires des particuliers. Ils visent de plus en plus souvent les téléphones portables.
- ***le carding :*** vente de données personnelles captées par des organisations criminelles, principalement sur le Darknet.
- ***le jackpotting :*** connexion d'un ordinateur équipé d'un logiciel ad hoc sur un distributeur de billets, pour en prendre le contrôle et ordonner la remise des fonds pouvant aller jusqu'à 120 000 euros.

Les réseaux d'information, comme vecteur ou moyen de l'infraction

Les réseaux de communication sont le vecteur privilégié des organisations criminelles, en offrant un moyen de démultiplier le nombre de victimes, de s'immiscer dans leur sphère privée et d'agir à distance, dans une relative impunité.

- ***Les escroqueries astucieuses :*** escroqueries à la romance, chantages à la webcam, fausses annonces. Elles restent très présentes malgré l'action des politiques de prévention.
- ***La diffusion massive de contenus illicites*** sur le web (contenus pédopornographiques, apologie du terrorisme, incitation à la haine raciale ou religieuse, annonces de proxénétisme, diffusion de données personnelles).
- ***L'utilisation des réseaux sociaux par les trafiquants de stupéfiants*** qui ont adapté leur offre de distribution (« Ubershit »), ont été récemment favorisé par la numérisation de la société.
- ***La cyber-haine, (notamment terroriste)*** détourne les outils du web à des fins de propagande, d'intimidation et de harcèlement et s'immisce ainsi dans tous les aspects de la vie sociale.

Les enjeux :
- limiter la visibilité des contenus par des mesures de retrait, de blocage et de déréférencement ;
- identifier leurs auteurs pour casser le sentiment d'impunité favorisant le passage à l'acte ;
- lutter contre les prestataires de services techniques complaisants voire complices, qui permettent la diffusion de ces contenus illicites.

La cybercriminalité « à la demande »

La notion de *Cyber-crime as a Service* renvoie à la sous-traitance de produits et services contre rémunération sur le marché parallèle du Darkweb :
- accès à des systèmes compromis, bases de données de cartes de crédits volées ;
- organisation d'attaques en déni de service distribuées (DDOS) ;
- test de la détection par antivirus de logiciels malveillants.

Ce système permet aux concepteurs de logiciels malveillants de se positionner en retrait, en vendant leurs produits sur le darkweb, sans avoir à conduire eux-mêmes les attaques. Les organisations criminelles se chargent de la mise en œuvre, sans disposer de connaissances techniques spécifiques.

Exemple : EMOTET, le botnet le plus puissant du monde, démantelé par l'OCLCTIC

Ce logiciel malveillant, parmi les plus dangereux qui soit, était proposé à la location des cybercriminels pour installer d'autres types de logiciels malveillants. Une fois implanté sur une machine, il permettait d'en copier les données, de les exfiltrer ou d'y déposer des malwares. Dans la continuité de l'enquête ouverte par l'office, une vaste opération policière coordonnée par Europol a été menée en 2021 pour mettre hors service les serveurs de contrôle et interpeller le concepteur du botnet.

Les enjeux : imputer les actes criminels aux prestataires techniques et aux bénéficiaires des attaques, qu'il s'agisse d'individus isolés réalisant des gains faciles, d'organisations criminelles traditionnelles diversifiant leurs activités, d'entreprises désorganisant leurs concurrents, d'entités libertaires contestant la régulation du web ou d'États masquant leurs actions offensives sur le cyberespace.

2022-2027
Une réponse ambitieuse de la police nationale

+306 EFFECTIFS | **+2 450** SPÉCIALISTES FORMÉS | **+1** NOUVEL OFFICE ANTI-CYBERCRIMINALITÉ (OFAC)

Objectif n°1

Apporter une réponse judiciaire adaptée à toutes les formes de la cybercriminalité

Pour combattre efficacement les différentes facettes de la cybercriminalité, la police nationale rénove et renforce ses capacités d'enquête.

Cette montée en puissance suppose une réorganisation de toutes les structures cyber de la police nationale pour créer – à travers la filière cyber renforcée et animée par le nouvel office anti-cybercriminalité (OFAC) – un continuum d'action de la police nationale sur le territoire et à l'international.

Monter en compétence tous les acteurs de la filière cyber

Il s'agit autant de créer des réflexes cyber à tous les niveaux d'investigation pour lutter contre la cybercriminalité de masse que d'acquérir un savoir-faire d'experts pour traiter le haut du spectre en diversifiant les compétences et les profils.

- **Accroître** les contenus cyber des formations initiales des commissaires de police, officiers de police et gardiens de la paix.
- **Recruter** par la voie contractuelle des profils nouveaux et complémentaires : ingénieurs, analystes, informaticiens.
- **Professionnaliser** les formations cyber avec la spécialisation d'une école de police dans le domaine cyber avec une formation, des moyens et des matériels renforcés pour repérer les profils spécifiques et la participation à l'école cyber annoncée par le Président de la République.

Renforcer les capacités des services d'enquête cyber et généralistes

- **+1000 PRIMO-INTERVENANTS** en cybercriminalité (PICC) pour réaliser les analyses numériques de premier niveau.
  744 aujourd'hui → 1 744 demain
- **+600 INVESTIGATEURS EN CYBERCRIMINALITÉ** (ICC) pour effectuer les analyses forensic.
  909 aujourd'hui → 1 509 demain
- **+750 CYBERPATROUILLEURS** formés et habilités à l'enquête sous pseudonyme (ESP).
  230 aujourd'hui → 980 demain
- **+100 SCIENTIFIQUES SPÉCIALISÉS EN CRIMINALISTIQUE NUMÉRIQUE** pour mettre en évidence les traces numériques.
  185 aujourd'hui → 285 demain

Réorganiser la filière cyber en confiant son pilotage au nouvel Office anti-cybercriminalité

Cette nouvelle organisation en filière doit permettre de traiter l'ensemble des infractions cyber en tous points du territoire national. Pour toute assistance opérationnelle ou procédurale, les structures cyber déclinées à chaque échelle (central, zonal, départemental) sont des « guichets uniques » à disposition des enquêteurs pour les appuyer et traiter l'aspect cyber de leurs dossiers.

AU NIVEAU NATIONAL

Transformer l'office central de la lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) qui devient l'office anti-cybercriminalité (OFAC), chef de file de la lutte contre la cybercriminalité sur le modèle OFAST.

4 MISSIONS :

DÉTECTER, RENSEIGNER, ENQUÊTER ET APPUYER

+86
PERSONNELS

UNE ACTION JUDICIAIRE RECENTRÉE SUR LE TRAITEMENT DES INFRACTIONS DU HAUT DU SPECTRE : LES CYBERATTAQUES LES PLUS COMPLEXES ET LES OFFRES DE CYBER-SERVICES CRIMINELS.

AU NIVEAU TERRITORIAL

Renforcer les territoires pour appuyer les enquêteurs

+11 ANTENNES CYBER

6 AU NIVEAU ZONAL
1 À VERSAILLES
ET 4 DANS LES TERRITOIRES ULTRA-MARINS

+45 DÉTACHEMENTS D'ANTENNES

AU NIVEAU DÉPARTEMENTAL, RELAIS TERRITORIAUX DE L'OFFICE

+220
PERSONNELS

+ CRÉATION DE POINTS DE CONTACT EXPERTS (ICC)

AU NIVEAU DÉPARTEMENTAL POUR RECEVOIR TOUTES LES DEMANDES D'APPUI DES ENQUÊTEURS SUR LE VOLET CYBER DE LEURS DOSSIERS.

Objectif n°2

Protéger les citoyens, les entreprises et les collectivités

Assurer la sécurité de la population face à la menace cyber c'est d'abord, pour la police nationale, être en capacité de détecter, à travers le renseignement criminel, les cyber-menaces du quotidien comme celles plus exceptionnelles liées à l'organisation de grands évènements.

Soucieuse en permanence de consolider son lien avec la population, la police nationale place aussi les usagers au cœur de son dispositif de lutte contre la cybercriminalité. Le volet prévention de ce plan a ainsi un double objectif : informer et sensibiliser la population sur les risques cyber, prendre en charge et accompagner les victimes de cyber-infractions.

Améliorer la détection des cyber-menaces

Piloter le renseignement cybercriminel avec la création d'un pôle renseignement intégrant SIRASCO CYBER :

- → Production régulière d'états de la menace cybercriminelle et des phénomènes émergents en lien avec les autres acteurs du renseignement : le renseignement territorial, l'ANSSI, la DGSI, la DGGN et la préfecture de police.
- → Enrichissement des enquêtes par la production d'analyses opérationnelles.

Anticiper une attaque cyber d'ampleur dans le cadre des grands évènements (Coupe du monde de rugby 2023, Jeux Olympiques 2024) :

- → Construction par l'office d'un plan d'attaque cyber pour la police nationale avec un volet dédié à la coopération opérationnelle de l'ensemble des partenaires extérieurs.
- → Participation aux instances de gestion de crises mises en place dans le cadre du déclenchement du plan PIRANET.

Renforcer la prévention des cyber-menaces en consolidant les liens avec la population

Développer, en lien et en cohérence avec le dispositif « action contre la cybermalveillance » (ACYMA), des actions de prévention et des campagnes d'information à destination des usagers dans leurs pratiques digitales quotidiennes et des acteurs du monde économique :

- → Créer une nouvelle application sur Néo 2 pour permettre à tous les policiers au contact du public de le sensibiliser sur les bons réflexes à adopter pour se prémunir des risques cyber, à partir des contenus déjà proposés par ACYMA.
- → Étendre le réseau cyber-menace (RECYM), composé de spécialistes cyber actifs et issus de la réserve opérationnelle de la police, pour accompagner les ETI, TPE, PME et les collectivités territoriales face aux menaces cyber liées à leurs activités professionnelles.

Accompagner les victimes de cyber-attaques pour leur apporter une réponse rapide et adaptée

- → Mise en place du « 17 cyber » et communication renforcée sur la plateforme téléphonique info-escroqueries pour orienter les victimes de cyber-infractions.
- → Extension de la plainte en ligne avec l'élargissement du champ infractionnel de THESEE aux faux placements et la mise en place de bornes dédiées dans les commissariats pour multiplier les possibilités offertes aux victimes cyber de déposer plainte en ligne.

Objectif n°3

Améliorer la coordination et la coopération avec les autres acteurs engagés dans la lutte contre la cybercriminalité

En tant que chef de file de la filière cyber de la police nationale et en tant que coordonnateur opérationnel du renseignement criminel et de la réponse judiciaire apportée à la cybercriminalité, l'office ambitionne de jouer un rôle pivot pour améliorer la coordination entre les différents services étatiques à l'échelle nationale ainsi qu'avec les instances européennes et internationales.

La menace cyber étant globale, son traitement dépasse largement le cadre institutionnel ; aussi, ce plan prévoit également de développer les actions de partenariats avec l'ensemble des acteurs concernés, universitaires, industriels.

Mieux se coordonner pour rendre l'action étatique plus efficiente face à la cybercriminalité

Sur le territoire national, renforcer le rôle de pilote de l'office en charge de l'animation, de la centralisation et de la coordination opérationnelle de la lutte contre cette criminalité :

- → Développement de la composition interministérielle de l'OFAC notamment avec la DGGN et la DGDDI.
- → Renforcement des échanges d'informations cybers interministériels et inter-services : préfecture de police de Paris, DGSI, ComCyberGend, l'ANSSI, le parquet de Paris...
- → Mise en place du « CJUD OPS », nouvelle instance interministérielle de partage d'information entre les services de renseignement et les services judiciaires.

À l'échelle européenne et internationale, poursuivre l'investissement de l'OFAC comme point de contact 24/7 et meneur des initiatives de coopération :

- → Augmentation du nombre d'officiers de liaison cyber présents à l'étranger
- → Participation active de l'office à des projets européens d'ampleur et aux formations internationales (CEPOL).

Coopérer davantage avec les acteurs privés pour renforcer l'efficacité de la réponse étatique à cette menace

Développer les partenariats avec les acteurs économiques privés :

- → Participation active de l'OFAC au Campus-cyber en partageant certaines productions du SIRASCO sur l'état de la menace
- → Etablissement de liens, via des partenariats publics/privés avec les acteurs du monde de l'industrie et des nouvelles technologies pour enrichir la connaissance opérationnelle de la police nationale et permettre l'accès à de nouveaux moyens techniques performants.

Renforcer les liens avec les acteurs universitaires de pointe :

- → Développement de partenariats de formation avec les universités et les secteurs privés pour accéder à des enseignements spécifiques cyber non proposées dans la police et des formations de pointe dispensées par des entreprises spécialisées.
- → Conduite de projets de partenariats autour de projets de recherche en matière cyber.

Les 37 mesures opérationnelles du plan

Axe I
Une cyber police mieux organisée et plus efficace

MESURE N°1	Organiser l'office anti-cybercriminalité (OFAC) autour de 4 missions essentielles : détecter, renseigner, enquêter et appuyer.
MESURE N°2	Axer le traitement judiciaire de **l'OFAC** sur les cyberattaques les plus complexes (ex : les rançongiciels) et sur les nouveaux contentieux liés notamment aux offres de cyber services criminels en développant la synergie des compétences entre ingénieurs et enquêteurs ainsi qu'en s'appuyant sur l'expertise du **laboratoire central de criminalistique numérique du service national** de police scientifique (SNPS)
MESURE N°3	Coordonner, piloter la filière cyber de la PN et appuyer les services de terrain : • création de 6 antennes zonales cyber, d'une antenne cyber à Versailles et de 4 antennes cyber dans les territoires ultra-marins. Chaque antenne sera composée d'un département d'enquête numérique (ICC) et d'un département de criminalistique numérique (agents des SCN du SNPS). Elles seront placées sous l'autorité fonctionnelle de l'office et exerceront elles-mêmes une autorité fonctionnelle sur les structures cyber situées sur leur ressort pour : être le relais territorial de l'office dans le traitement des cyberattaques (**enquêter**) ; assurer l'assistance cyber de tous les enquêteurs de la police nationale dans le traitement de tout type d'infraction (**appuyer**) ; encadrer l'action locale du réseau des « référents cybermenaces » (RECYM) (**renseigner**) ; coordonner et suivre l'activité des agents cyber (ICC, ESP, agents des SCN) sur leur ressort (**appuyer**). • création de 45 détachements d'antennes positionnés à l'échelon départemental, organisés selon le même modèle que les antennes (agents SCN et ICC) et disposant de niveaux d'action variables selon le lieu d'implantation et le dimensionnement de la structure

MESURE N°3	• création de **points de contact d'experts (ICC)** dans tous les autres départements avec une mission d'appui. Cette organisation territoriale crée **un maillage de guichets uniques**, pilotés par l'OFAC, pour recevoir les demandes cyber des enquêteurs et les accompagner dans leurs cyber investigations.
MESURE N°4	Développer l'aide cyber de proximité pour répondre aux besoins en termes de cyber-investigation et de criminalistique numérique des enquêteurs généralistes.
MESURE N°5	Poursuivre l'investissement de l'OFAC en matière de **coopération opérationnelle** et stratégique à l'échelle **européenne et internationale :** • renforcer le nombre d'ODL cyber présents à l'étranger • développer la participation active de l'office à des projets européens d'ampleur (ex : driver EMPACT), • accroître la participation de l'office (formateurs) aux différentes formations internationales (CEPOL) et aux travaux de conception de stratégie de renforcement des capacités.
MESURE N°6	Accroître les capacités d'exploitation de données de masse et de mutualisation des moyens et des compétences par l'intermédiaire d'une présence forte de l'OFAC à Rennes **(plateau technique cyber)** aux côtés de l'ANSSI, de la DGSI, du ComCyber et du ComCyber Gend.
MESURE N°7	Développer les **partenariats publics/privés** et l'échange d'information entre les services actifs dans l'écosystème cyber en affectant des personnels de l'OFAC (actifs et contractuels) au Campus Cyber.

MESURE N°8	Développer les partenariats entre l'OFAC et le monde de **l'industrie et des nouvelles technologies** : • participation active de l'OFAC à l'interCERT et au Campus-cyber ; • diffusion et partage de certaines productions du SIRASCO • intervention conjointe lors des sessions de formation continue ; • développement de liens directs par l'intermédiaire du RECYM
MESURE N°9	Anticiper une réponse judiciaire de **crise** en cas d'attaque cyber d'ampleur impliquant la construction d'un plan d'attaque cyber (type plan attentat) pour la police nationale.
MESURE N°10	Participer aux instances de gestion de crises mises en place dans le cadre du déclenchement du plan **PIRANET** ainsi qu'à la réflexion sur la refonte du volet judiciaire du plan.

Axe II
Une cyber police qui détecte, partage et protège

MESURE N°11	Renforcer le rôle de pilotage de l'office en matière de renseignement cybercriminel en y créant un pôle renseignement intégrant un **SIRASCO CYBER** avec une triple mission : 1/ enrichir les enquêtes par la production d'analyses opérationnelles, pour initier ou étayer des enquêtes ; 2/ produire des états de la menace réguliers ; 3/ développer le partenariat avec le secteur privé et le monde de la recherche.
MESURE N°12	Mise en place d'une instance interministérielle de partage entre les services de renseignement et les services judiciaires avec la création d'un « **CJUD OPS** » et ses déclinaisons et dynamiser leurs échanges.

MESURE N°13	Promouvoir **PHAROS** et **THESEE** comme outils de criblage, de déconfliction et de rapprochements à disposition de tous les services.
MESURE N°14	Mieux intégrer la **filière renseignement** de la police nationale dans la communauté cyber (temps d'échange formalisé au niveau central et territorial sur l'état de la menace, offre de prestations forensique au SCRT, point de contact SCRT à PHAROS).
MESURE N°15	Renforcer les échanges d'informations cyber interministériels et inter-services en développant la **composition interministérielle** de l'office (modèle OFAST) avec la DGFIP et la DGGN.
MESURE N°16	Recruter, par la voie contractuelle, des profils nouveaux et complémentaires à ceux issus des filières classiques de la police nationale. Cette mesure permettra de partager des savoirs et de **diversifier les profils des hauts potentiels à la filière cyber**. Dans cette optique, participer et intervenir dans les salons étudiants et écoles d'ingénieurs pour attirer des profils cyber vers la police.
MESURE N°17	Développer le dispositif **17 cyber** pour apporter une réponse rapide et adaptée aux victimes de cyber-attaques.
MESURE N°18	Élargir le champ infractionnel de **THESEE** notamment aux faux placements (fraude à l'investissement, escroqueries aux congés de formations etc).
MESURE N°19	Développer les possibilités offertes aux usagers pour déposer plainte en ligne sur THESEE avec la mise en place de **bornes dédiées dans les commissariats** permettant un accès aux téléservices PN.

MESURE N°20	Développer les liens du **CSIRT-PJ avec l'inter-CERT et les CSIRT régionaux** afin de sensibiliser les partenaires de la cybersécurité aux enjeux de la judiciarisation et accroître le recueil d'éléments d'enquête.
MESURE N°21	Renforcer les actions de **prévention à destination des usagers** dans leurs pratiques digitales quotidiennes et développer le partenariat avec les entités (cybermalveillance, association e-enfance) en charge de la production de messages de prévention des risques à la population.
MESURE N°22	Développer le dispositif du réseau RECYM pour accompagner les **ETI, TPE, PME** et les collectivités territoriales face aux risques inhérents au cyberespace : • intégrer le réseau cyber-menace (RECYM) aux antennes cyber et faire des coordonnateurs RECYM le point de contact PN unique pour les partenaires institutionnels et privés ; • recruter des experts parmi les futurs réservistes de la réserve opérationnelle.
MESURE N°23	Cadrer l'action du RECYM pour prévoir une interaction entre les experts cyber et les référents sûretés.

Axe III
Une police plus cyber

MESURE N°24	Créer une application de type « boîte à outil cyber » accessible sur NEO 2 permettant de répondre aux besoins des policiers de terrain et des enquêteurs en perquisition.
MESURE N°25	Accroître significativement la part de **formation** cyber dans toutes les formations initiales (FI).
MESURE N°26	Ajout d'une formation complémentaire sur les bases de l'investigation numérique (BIN) dans le **module d'adaptation au premier emploi** des élèves gardiens de la paix s'orientant vers une filière judiciaire.
MESURE N°27	**Spécialiser une école de police** dans le domaine cyber avec une formation, des moyens et des matériels renforcés, créant ainsi naturellement un vivier cyber ainsi que la possibilité de permettre le recrutement dans les services d'investigation dès la sortie d'école de profils avec une compétence cyber spécifique.
MESURE N°28	Participation de la police nationale à **l'école cyber** annoncée par le Président de la République avec la détermination, en commun avec la gendarmerie nationale, d'un socle de formations.
MESURE N°29	Accroître le nombre de **PICC** (+1 000) ainsi que de **cyber-patrouilleurs** (+750) afin d'être en capacité collective de faire face à l'augmentation importante de la dimension cyber des enquêtes pour les services généralistes.
MESURE N°30	**Harmoniser et moderniser les formations** dédiées à l'investigation technique et numérique.

MESURE N°31	Réorganiser l'offre de formation destinée à tous les policiers en matière de recherche en **sources ouvertes**, darknet, crypto-monnaies, enquêtes sous pseudonyme et équiper les 21 salles de formation en investigation numérique.
MESURE N°32	Ouvrir, à l'ensemble du ministère de l'intérieur, le **forum** *R@cine* qui permet aux enquêteurs formés en cyber d'échanger sur leurs pratiques.
MESURE N°33	Créer des modules de formation dédiés aux besoins des services spécialisés.
MESURE N°34	Développer des partenariats de formation avec les **universités, les secteurs privés** ou associatifs pour accéder à des formations spécifiques non réalisées dans le cursus DCRFPN.
MESURE N°35	Disposer d'un budget dédié pour garantir l'accès à des **formations de pointe dispensées** par des entreprises spécialisées. L'inscription à ces formations sera subordonnée à un engagement minimum d'exercice dans la filière cyber de la PN.
MESURE N°36	**Cartographier les formations et les compétences de la police nationale** sur les différents territoires pour permettre aux services de solliciter plus facilement une formation ou de l'aide cyber. **Assurer un partage avec la gendarmerie.**
MESURE N°37	Développer l'utilisation d'un **logiciel commun** pour 1/ assurer le suivi des matériels, formations et de l'activité des antennes. 2/ produire des statistiques à partir d'indicateurs, élaborés en lien avec le SSMSI, sur les investigations numériques et la lutte contre la cybercriminalité.

LA POLICE NATIONALE
S'ENGAGE AUPRÈS DES VICTIMES

Réalisation graphique : SICOP