

LES CAHIERS DU CERCLE AVENIR & PROGRÈS

Collection « Cohésion nationale »

Première édition · 2026

Cahier numéro 2

La Sécurité

Garantir la cohésion nationale par la sécurité



SOMMAIRE

AVANT-PROPOS.....	5
POURQUOI CE CAHIER ?.....	7
SYNTHÈSE EXÉCUTIVE.....	9
Les principaux constats	9
Les propositions structurantes	10
Les propositions d'avenir : préparer la sécurité de demain.....	11
Les trois convictions de la Commission	12
Regards européens.....	12
Ce que la Commission retient	16
LE RAPPORT DE LA COMMISSION.....	18
PREMIÈRE PARTIE - Comprendre les nouvelles formes de l'insécurité.....	18
CHAPITRE 1 - La sécurité commence par l'autorité.....	19
Une crise de confiance qui fragilise la sécurité	19
Une banalisation préoccupante des violences.....	20
La transmission, premier rempart contre l'insécurité	20
Restaurer une culture de la responsabilité	20
CHAPITRE 2 - Les forces de sécurité : des moyens importants, une efficacité à renforcer	21
Une organisation devenue complexe.....	21
Redonner du temps au terrain	22
Préserver l'engagement des femmes et des hommes	22
Adapter les compétences aux nouvelles menaces	22
Faire de l'efficacité le premier objectif.....	23
CHAPITRE 3 - Justice : restaurer l'efficacité de la chaîne pénale.....	23
Une chaîne pénale qui doit gagner en fluidité.....	23
Une justice plus rapide pour une justice plus crédible.....	24
Donner toute sa force à l'exécution des peines.....	24
Moderniser la politique pénitentiaire.....	24
Renforcer la coopération entre tous les acteurs.....	25
Restaurer la confiance dans la justice.....	25
Conclusion de la première partie	26
DEUXIÈME PARTIE - La sécurité du 21^{ème} siècle : vers une approche globale	27

CHAPITRE 4 - Comprendre la révolution cyber.....	29
Pourquoi le cyber change la nature même de la sécurité	29
Une mutation profonde des menaces	29
Le risque cyber : un risque systémique.....	30
Une cybercriminalité devenue industrielle	31
Un enjeu économique majeur	31
Un enjeu de souveraineté nationale	32
CHAPITRE 5 - L'État face à la cybermenace.....	32
Une organisation progressivement structurée	32
Une stratégie nationale désormais affirmée.....	33
Une gouvernance progressivement structurée	33
Une coopération devenue indispensable	33
Des moyens renforcés mais des fragilités persistantes.....	34
Les défis des prochaines années	34
CHAPITRE 6 - Former une Nation cyber-résiliente.....	35
Le facteur humain, premier rempart contre la cybermenace.....	35
Faire de la formation une priorité stratégique	35
Développer une véritable culture de cybersécurité.....	36
Adapter les compétences aux responsabilités	36
Accompagner durablement les territoires.....	37
Sensibiliser l'ensemble de la société	37
Les compétences, nouvel enjeu de souveraineté.....	37
Conclusion de la deuxième partie	38
UNE AMBITION POUR 2030 - Construire une France plus sûre, plus résiliente et plus souveraine	40
LES RECOMMANDATIONS DE LA COMMISSION	42
Cinq recommandations prioritaires	42
Les principales actions proposées	43
1. Simplifier l'action des forces de sécurité	43
2. Accélérer le fonctionnement de la chaîne pénale.....	43
3. Développer une véritable politique de prévention.....	43
4. Renforcer la résilience numérique de la Nation	44
5. Consolider la souveraineté technologique.....	44
CONCLUSION	45
ANNEXES	46

Annexe 1 — La Commission : méthode de travail et composition.....	46
Annexe 2 — Les auditions et contributions ayant nourri les travaux de la Commission.....	47
Annexe 3 — Les principaux textes juridiques de référence.....	49
Annexe 4 — Bibliographie sélective.....	52

AVANT-PROPOS

Assurer la sécurité des Français est la première des libertés. Elle constitue la mission première de l'État et l'un des fondements du pacte républicain. Sans sécurité, il ne peut y avoir ni confiance, ni justice, ni développement économique, ni cohésion nationale.

Pourtant, la sécurité ne peut plus être appréhendée aujourd'hui comme hier.

La France est confrontée à une évolution profonde des menaces. À la délinquance du quotidien s'ajoutent désormais le terrorisme, les violences urbaines, les trafics organisés, les atteintes aux élus, les cyberattaques, les manipulations informationnelles et les attaques contre les infrastructures essentielles de notre pays. Les frontières entre sécurité intérieure, justice, défense, renseignement et cybersécurité deviennent chaque jour plus étroites.

Face à ces mutations, le Cercle Avenir & Progrès a souhaité consacrer un Cahier à la sécurité.

Notre objectif n'est pas d'ajouter une contribution de plus à un débat souvent passionnel. Il est de proposer une analyse fondée sur les faits, les retours d'expérience des professionnels et les données disponibles, afin d'identifier les évolutions nécessaires pour renforcer l'efficacité de l'action publique.

Les travaux de la Commission conduisent à un constat simple : la France ne souffre pas uniquement d'un manque de moyens. Elle souffre surtout d'une difficulté à transformer les moyens qu'elle consacre à la sécurité en une présence effective, visible et continue sur le terrain, ainsi qu'en une réponse rapide, cohérente et crédible de l'ensemble de la chaîne de sécurité et de justice.

Ils montrent également que la sécurité ne relève plus des seules forces de l'ordre. Elle mobilise l'ensemble de la puissance publique. L'éducation, la justice, la politique pénitentiaire, la prévention, le numérique, la cybersécurité, mais aussi la responsabilité des familles, des collectivités territoriales, des entreprises et des citoyens participent désormais d'une même ambition : protéger durablement la société.

La sécurité constitue aujourd'hui un enjeu majeur de cohésion nationale. Lorsqu'elle recule, c'est la confiance dans les institutions qui s'affaiblit, le sentiment d'appartenance à la communauté nationale qui se fragilise et les fractures territoriales et sociales qui s'accroissent. À l'inverse, une politique de sécurité efficace contribue à garantir l'exercice des libertés, à restaurer la confiance dans l'action publique et à renforcer le pacte républicain.

Ce Cahier rassemble les travaux de la Commission Sécurité du Cercle Avenir & Progrès. Il dresse un état des lieux de la sécurité intérieure et de la cybersécurité en France, analyse les transformations profondes auxquelles notre pays est confronté et formule des propositions destinées à améliorer l'efficacité de notre politique de sécurité.

Nous sommes convaincus que la sécurité n'est pas seulement une politique publique parmi d'autres, mais l'une des conditions essentielles de la liberté, de la confiance et de la cohésion nationale.

Jean-Luc Scemamma
Président du Cercle Avenir & Progrès

* * *

POURQUOI CE CAHIER ?

Assurer la sécurité des citoyens constitue la première mission de l'État. Elle est la condition première de l'exercice des libertés, de la confiance dans les institutions et du fonctionnement de la vie démocratique. Sans sécurité, il ne peut y avoir ni justice pleinement effective, ni développement économique durable, ni cohésion nationale.

Longtemps, la sécurité a été appréhendée principalement à travers la lutte contre la délinquance, le maintien de l'ordre public et la protection des personnes et des biens. Ces missions demeurent essentielles. Elles ne suffisent cependant plus à répondre aux défis auxquels notre pays est aujourd'hui confronté.

Les menaces ont profondément changé de nature. À la délinquance du quotidien s'ajoutent désormais le terrorisme, les trafics internationaux, les violences contre les représentants de l'autorité, les ingérences étrangères, les manipulations de l'information, les cyberattaques ou encore les atteintes aux infrastructures critiques. La frontière entre sécurité intérieure, justice, défense, renseignement et cybersécurité devient de plus en plus ténue. La sécurité est devenue un enjeu global, qui mobilise l'ensemble de la puissance publique.

Cette évolution conduit également à dépasser une idée largement répandue : la sécurité ne dépend pas uniquement des forces de l'ordre. Elle repose aussi sur l'efficacité de la chaîne pénale, sur la capacité de l'État à protéger ses infrastructures numériques, sur le rôle de l'école dans la transmission des règles communes, sur l'accompagnement des familles, sur la prévention, sur les collectivités territoriales, sur les entreprises et, plus largement, sur la responsabilité de chacun. La sécurité est devenue une responsabilité collective.

Les travaux de la Commission conduisent également à un constat qui mérite d'être souligné. La France ne souffre pas principalement d'un manque de moyens. Elle dispose de forces de sécurité reconnues, d'une justice indépendante, de services de renseignement performants et d'une stratégie nationale de cybersécurité ambitieuse. Le défi réside davantage dans notre capacité à coordonner ces moyens, à simplifier leur organisation et à les transformer en une action plus visible, plus réactive et plus efficace au service des citoyens.

Le Cercle Avenir & Progrès a souhaité aborder cette question avec la même méthode que pour l'ensemble de ses Cahiers : partir des faits, confronter les analyses des experts aux réalités du terrain, écouter les praticiens, comparer les expériences et formuler des propositions concrètes, sans tabou ni dogmatisme.

Car la sécurité n'est pas seulement une politique publique parmi d'autres.

Elle est l'un des fondements de notre pacte républicain.

Elle garantit l'exercice des libertés, protège la confiance des citoyens dans leurs institutions et conditionne notre capacité à faire société.

À l'heure où les menaces se diversifient et où les attentes des Français n'ont jamais été aussi fortes, repenser notre politique de sécurité ne consiste pas seulement à

répondre aux urgences du présent. Il s'agit aussi de préparer une France plus résiliente, plus souveraine et plus confiante face aux défis du 21^{ème} siècle.

* * *

SYNTHÈSE EXÉCUTIVE

Les principaux constats

Les travaux de la Commission conduisent à un constat majeur : la sécurité ne peut plus être pensée comme hier. Les menaces ont changé de nature, les attentes des citoyens se sont renforcées et l'efficacité de l'action publique dépend désormais de la capacité de l'État à coordonner l'ensemble de ses moyens. Six enseignements se dégagent.

1. La sécurité est le premier fondement du pacte républicain

La sécurité ne constitue pas une politique publique parmi d'autres. Elle garantit l'exercice des libertés, la confiance dans les institutions, l'attractivité des territoires et la cohésion nationale. Sans sécurité, il ne peut y avoir ni État de droit pleinement effectif, ni vie démocratique apaisée.

2. Les menaces du 21^{ème} siècle imposent une approche globale

Aux violences du quotidien s'ajoutent désormais le terrorisme, les trafics organisés, les cyberattaques, les manipulations informationnelles, les ingérences étrangères et les attaques contre les infrastructures critiques. La distinction entre sécurité intérieure, justice, défense, renseignement et cybersécurité s'estompe progressivement. La sécurité est devenue un enjeu global de résilience nationale.

3. L'enjeu n'est plus seulement celui des moyens, mais de leur efficacité

La France dispose de forces de sécurité reconnues, d'une justice indépendante, de services spécialisés performants et d'investissements importants. Pourtant, ces moyens peinent encore à produire une présence visible, une réponse rapide et une action pleinement coordonnée. Le défi est désormais celui de la performance collective.

4. La sécurité est une responsabilité partagée

Les forces de l'ordre ne peuvent agir seules. Justice, administration pénitentiaire, éducation, collectivités territoriales, entreprises, familles et citoyens contribuent chacun à la protection de la société. La prévention, la transmission des règles communes et la restauration de l'autorité participent pleinement de la politique de sécurité.

5. La cybersécurité est devenue un enjeu majeur de souveraineté

Le cyberspace est désormais un espace de confrontation stratégique. La protection des données, des infrastructures critiques, des administrations, des entreprises et des collectivités conditionne la continuité de l'État, la compétitivité économique et l'indépendance nationale. La cybersécurité est devenue un pilier de la sécurité nationale.

6. Restaurer la confiance est la finalité de la politique de sécurité

Une politique de sécurité efficace ne se mesure pas uniquement au nombre de moyens engagés ou d'infractions constatées. Elle se mesure à la confiance qu'elle

inspire. Restaurer la crédibilité de l'action publique, garantir une réponse lisible et renforcer le lien entre les citoyens et leurs institutions constituent désormais des objectifs à part entière.

Les propositions structurantes

Cinq priorités pour construire une politique de sécurité plus efficace, plus résiliente et plus souveraine

Les travaux de la Commission montrent que la France ne manque ni de compétences, ni d'engagement, ni de moyens. Le principal défi consiste désormais à mieux coordonner l'action publique, à adapter notre modèle de sécurité aux menaces du 21^{ème} siècle et à restaurer la confiance des citoyens. Cinq priorités structurent cette ambition.

1. Faire de l'efficacité opérationnelle la première exigence de la sécurité intérieure

Renforcer la présence des forces de sécurité sur le terrain, simplifier les procédures, améliorer la coordination entre les services et recentrer les moyens sur les missions opérationnelles afin d'offrir aux citoyens une sécurité plus visible, plus réactive et plus efficace.

2. Restaurer la crédibilité de la chaîne pénale

Garantir une réponse judiciaire plus rapide, plus lisible et effectivement exécutée en renforçant la coopération entre les forces de sécurité, la justice et l'administration pénitentiaire, afin de conforter l'autorité de l'État de droit.

3. Construire une politique de sécurité fondée sur la prévention et la responsabilité

Agir en amont des violences en mobilisant l'école, les familles, les collectivités territoriales, les associations et l'ensemble des acteurs de terrain, afin de prévenir les ruptures, lutter contre la récidive et renforcer la cohésion sociale.

4. Faire de la cybersécurité un pilier de la souveraineté nationale

Intégrer pleinement la cybersécurité à la politique de sécurité nationale en renforçant les capacités de prévention, de détection et de réaction face aux menaces numériques, tout en développant une véritable culture de la résilience.

5. Affirmer une souveraineté française et européenne face aux nouvelles menaces

Développer les technologies souveraines, soutenir une filière industrielle de cybersécurité, renforcer les compétences stratégiques et approfondir les coopérations européennes afin de réduire les dépendances critiques et de protéger durablement les intérêts de la Nation.

Les propositions d'avenir : préparer la sécurité de demain

Au-delà des mesures destinées à améliorer le fonctionnement actuel de notre système de sécurité, la Commission invite à préparer un nouveau modèle capable de répondre aux mutations profondes du 21^{ème} siècle. Face à des menaces plus diffuses, plus hybrides et plus rapides, la France doit faire évoluer sa doctrine de sécurité autour de cinq orientations d'avenir.

1. Faire de la résilience le nouveau modèle de sécurité nationale

La sécurité ne peut plus être conçue comme une simple capacité de réaction aux crises. Elle doit permettre à la Nation d'anticiper les menaces, d'en limiter les effets et d'assurer la continuité de ses fonctions essentielles. Cette ambition suppose d'intégrer pleinement la prévention, la justice, le renseignement, la cybersécurité, la protection civile, l'industrie, l'éducation et les infrastructures critiques dans une stratégie nationale de résilience.

2. Construire une véritable culture nationale de sécurité

La sécurité ne relève plus des seuls services spécialisés. Elle devient une responsabilité partagée entre l'État, les collectivités territoriales, les entreprises, les associations et les citoyens. Développer une culture commune du risque, de la prévention et de la résilience constitue désormais un enjeu majeur de cohésion nationale et de souveraineté.

3. Piloter la sécurité par la performance et la confiance

L'efficacité des politiques de sécurité ne peut plus être appréciée au seul regard des moyens engagés. Elle doit être évaluée à partir de leurs résultats concrets : présence opérationnelle, rapidité de la réponse publique, exécution des décisions judiciaires, résilience des organisations, qualité du service rendu et confiance des citoyens dans leurs institutions.

4. Faire des territoires les premiers acteurs de la résilience

Les collectivités territoriales sont en première ligne face aux crises sécuritaires, sanitaires, climatiques ou numériques. Leur capacité d'anticipation, de coordination et de continuité des services publics constitue un élément essentiel de la résilience nationale. La Commission appelle à renforcer leurs compétences, leurs moyens et leur articulation avec l'État.

5. Inscrire l'anticipation au cœur de l'action publique

Dans un environnement marqué par l'accélération des transformations technologiques et géopolitiques, la sécurité doit reposer sur une capacité permanente d'anticipation. La prospective, le renseignement, l'intelligence artificielle, l'analyse des risques et la coopération européenne doivent permettre de détecter les vulnérabilités émergentes avant qu'elles ne se transforment en crises majeures.

Les trois convictions de la Commission

Au terme de ses travaux, la Commission retient trois convictions qui fondent l'ensemble de ses analyses et de ses propositions.

1. La sécurité est le premier devoir de la République

Avant d'être une politique publique, la sécurité est la condition d'exercice de toutes les autres. Elle garantit la liberté, protège l'État de droit, rend possible la cohésion nationale et fonde la confiance entre les citoyens et les institutions. Assurer la sécurité de tous constitue la première responsabilité de l'État républicain.

2. La sécurité du 21^{ème} siècle est globale et anticipatrice

Les menaces contemporaines dépassent largement le seul champ de la délinquance. Terrorisme, criminalité organisée, cyberattaques, manipulations informationnelles, crises sanitaires, risques climatiques et atteintes aux infrastructures critiques exigent une approche globale. La sécurité de demain ne reposera plus seulement sur la capacité à réagir, mais sur la capacité à anticiper, prévenir et renforcer la résilience de la Nation.

3. Une politique de sécurité efficace repose autant sur la confiance que sur la puissance publique

Les effectifs, les équipements et les technologies sont indispensables. Mais ils ne produisent pleinement leurs effets que s'ils s'accompagnent d'une organisation performante, d'une justice crédible, d'une coopération entre les acteurs et d'une confiance retrouvée entre les citoyens et leurs institutions. L'efficacité de la sécurité se mesure moins aux moyens engagés qu'à la capacité de l'État à protéger concrètement les Français.

La Commission est convaincue que la sécurité constitue aujourd'hui un bien commun. Sa préservation engage l'État, les collectivités territoriales, les entreprises, les associations et les citoyens eux-mêmes. C'est à cette condition que la France pourra construire une société plus libre, plus résiliente et plus souveraine.

Regards européens

Quelles politiques de sécurité pour demain ?

Les démocraties européennes sont confrontées à une transformation profonde de leur environnement de sécurité. À la délinquance et au terrorisme s'ajoutent désormais la criminalité organisée transnationale, les cyberattaques, les ingérences étrangères, les campagnes de désinformation et des crises susceptibles de fragiliser la continuité des services essentiels. Face à ces menaces hybrides, les États européens font évoluer leurs politiques de sécurité vers des approches plus globales, associant prévention, résilience, coordination des acteurs publics et privés et anticipation des risques.

Si chaque pays apporte des réponses adaptées à son histoire, à son organisation institutionnelle et à ses priorités, plusieurs expériences présentent un intérêt particulier pour la réflexion française. Elles montrent que l'efficacité d'une politique

de sécurité repose moins sur l'existence d'un modèle unique que sur quelques principes communs : une présence publique de proximité, une gouvernance territoriale efficace, une culture de la prévention et de la résilience, ainsi qu'une intégration croissante de la cybersécurité au cœur des politiques de souveraineté.

Les exemples qui suivent illustrent ces évolutions et mettent en lumière des pratiques dont la France peut utilement s'inspirer. (Commission européenne, *EU Security Union Strategy*, 2020 ; Europol, *SOCTA 2025*).

Le Royaume-Uni : rapprocher durablement la police des citoyens

Le Royaume-Uni a engagé depuis plusieurs décennies une politique visant à renforcer le lien entre les forces de police et la population. Sans remettre en cause les missions régaliennes de maintien de l'ordre et de lutte contre la criminalité, les autorités britanniques ont développé une approche fondée sur la proximité, la prévention et la responsabilité locale.

Les *Neighbourhood Policing Teams*, composées de policiers et d'agents de soutien, assurent une présence régulière dans les quartiers. Leur mission dépasse la seule intervention : elles entretiennent un dialogue permanent avec les habitants, identifient les préoccupations locales et travaillent en partenariat avec les collectivités, les établissements scolaires et les associations.

Parallèlement, le **College of Policing** a contribué à diffuser une véritable culture de l'évaluation des pratiques professionnelles. Les stratégies policières sont de plus en plus fondées sur l'analyse des données, l'expérimentation et la mesure de leur efficacité (*evidence-based policing*), afin d'améliorer l'allocation des moyens et la qualité du service rendu.

Cette approche n'a pas supprimé les difficultés rencontrées par les forces de sécurité britanniques, notamment en matière de violences urbaines ou de contraintes budgétaires. Elle illustre néanmoins l'intérêt d'une police davantage ancrée dans son territoire, attentive à la prévention et engagée dans une démarche d'amélioration continue.

Ce que la France peut en retenir : l'expérience britannique montre qu'une politique de sécurité efficace ne repose pas uniquement sur l'augmentation des effectifs ou le renforcement des sanctions. Elle suppose également une présence visible sur le terrain, un dialogue constant avec les citoyens, une coopération étroite avec les acteurs locaux et une culture de l'évaluation permettant d'adapter les politiques publiques aux résultats obtenus.

Les Pays-Bas : coordonner les acteurs au plus près des territoires

Les Pays-Bas ont fait le choix d'une police nationale organisée en unités régionales, tout en maintenant un pilotage étroit de la sécurité à l'échelle locale. Dans chaque territoire, le maire exerce l'autorité en matière d'ordre public, tandis que le procureur dirige l'action de la police judiciaire. Avec les responsables locaux de la police, ils se réunissent régulièrement afin de définir les priorités, d'adapter l'emploi des forces aux réalités du terrain et de coordonner la réponse publique (*Gouvernement des Pays-Bas ; ministère public néerlandais ; Commission européenne*).

Cette gouvernance territoriale permet d'associer plus directement les municipalités à la politique de sécurité. Elle repose également sur une coopération avec les services sociaux, les bailleurs, les établissements scolaires, les services de santé et les autres acteurs susceptibles d'identifier des situations de vulnérabilité ou des phénomènes criminels émergents.

Les autorités néerlandaises soulignent notamment le rôle de ces partenaires dans la prévention, la détection des activités illégales et la lutte contre la criminalité organisée (*Gouvernement des Pays-Bas ; Dutch National Police*).

Cette organisation favorise une approche intégrée de la sécurité. La réponse policière et pénale n'est pas isolée des politiques de prévention, d'action sociale ou d'aménagement territorial. Elle peut ainsi être adaptée à la nature des difficultés rencontrées localement, qu'il s'agisse de troubles à l'ordre public, de violences, de trafics ou de réseaux criminels.

Le modèle néerlandais ne supprime naturellement ni les tensions entre les acteurs ni les difficultés liées au partage de l'information. Il montre néanmoins qu'une police nationale peut conserver une forte capacité d'adaptation territoriale lorsque les responsabilités sont clairement réparties et que les décisions sont préparées conjointement par les autorités locales, la police et la justice.

Ce que la France peut en retenir : l'expérience néerlandaise souligne que l'efficacité d'une politique de sécurité dépend largement de la qualité de la coordination territoriale. Elle invite à mieux articuler l'action de l'État, des forces de sécurité, de l'autorité judiciaire, des collectivités territoriales et des acteurs sociaux, afin de construire des réponses adaptées aux réalités locales et d'agir simultanément sur la prévention, le maintien de l'ordre et la réponse pénale.

La Finlande : faire de la sécurité une responsabilité collective

La Finlande a développé un modèle de **sécurité globale** (*Comprehensive Security*) fondé sur une idée simple : la continuité des fonctions vitales de la société ne peut être garantie par l'État seul. Elle repose sur la coopération permanente des administrations, des collectivités territoriales, des entreprises, des organisations de la société civile et des citoyens (*Finnish Security Committee, **Security Strategy for Society**, 2025*).

Cette approche ne se limite ni à la défense nationale ni à la gestion des situations d'urgence. Elle englobe la continuité du fonctionnement de l'État, la sécurité intérieure, la défense, l'économie, les infrastructures, les services essentiels, la santé de la population et la capacité psychologique de la société à faire face aux crises. Pour chacune de ces fonctions, les responsabilités sont définies en amont et intégrées au fonctionnement ordinaire des institutions (*Finnish Security Committee*).

Le modèle finlandais repose également sur un réseau de coopération associant les pouvoirs publics, les entreprises, les universités, les associations et les opérateurs d'infrastructures critiques. Le partage de l'information, la définition d'objectifs communs et la préparation conjointe permettent de mobiliser rapidement les ressources nécessaires lorsqu'une crise survient (*Finnish Security Committee, **Comprehensive Security***).

La préparation constitue ainsi une politique permanente plutôt qu'une réponse ponctuelle aux crises. Les acteurs publics et privés participent à des exercices, élaborent des plans de continuité et entretiennent les compétences nécessaires pour faire face à des menaces diverses : catastrophes naturelles, crises sanitaires, attaques numériques, ruptures d'approvisionnement ou tensions géopolitiques. La résilience dépend autant de la qualité des organisations que de la capacité de la population à comprendre les risques et à adopter les comportements appropriés.

Cette approche est étroitement liée à la confiance entre les citoyens et les institutions. La sécurité est conçue comme un effort collectif dans lequel chacun connaît son rôle et peut contribuer, à son niveau, à la continuité de la société. Le modèle finlandais ne supprime naturellement ni les vulnérabilités ni les incertitudes. Il permet cependant de préparer les institutions et la population avant que la crise ne survienne, plutôt que de construire la réponse dans l'urgence.

Cette conception a également nourri les réflexions européennes récentes sur la préparation aux crises et la résilience collective, notamment dans le cadre des travaux relatifs à l'Union européenne de la préparation (*Commission européenne, **Safer Together: A Path Towards a Fully Prepared Union**, 2024*).

Ce que la France peut en retenir : l'expérience finlandaise montre que la résilience nationale ne repose pas uniquement sur les services spécialisés. Elle suppose une préparation continue, une répartition claire des responsabilités et une mobilisation coordonnée de l'État, des collectivités territoriales, des entreprises, des associations et des citoyens. Elle invite la France à développer une véritable culture nationale de la prévention et de la résilience, fondée sur la formation, les exercices réguliers, les plans de continuité et la participation de l'ensemble de la société.

L'Estonie : faire de la souveraineté numérique un choix stratégique

L'Estonie a fait du numérique l'un des fondements de son organisation administrative et de son développement économique. La très large dématérialisation des services publics lui a permis de simplifier les démarches, de fluidifier les échanges d'informations et de rapprocher l'administration des citoyens. Elle a également créé une dépendance forte au bon fonctionnement et à la sécurité des infrastructures numériques.

Les cyberattaques coordonnées qui ont frappé le pays au printemps 2007 ont constitué un tournant. Pendant plusieurs semaines, des institutions publiques, des médias, des banques et des services en ligne ont été visés par des attaques destinées à perturber leur fonctionnement. Cette crise a conduit l'Estonie à renforcer son cadre juridique, ses capacités opérationnelles et la coordination entre les administrations, les entreprises et les spécialistes de la cybersécurité (OTAN-CCDCOE, ***Analysis of the 2007 Cyber Attacks Against Estonia*** ; ENISA).

L'Estonie a progressivement intégré la cybersécurité à l'ensemble de sa stratégie nationale. La protection des services numériques n'y est pas considérée comme une simple responsabilité technique. Elle participe de la continuité de l'État, de la protection des infrastructures critiques, de la défense nationale et du maintien de la confiance des citoyens dans les institutions. Sa stratégie de cybersécurité 2024-2030 vise ainsi à garantir la fiabilité et la résilience des services numériques, y

compris dans un environnement sécuritaire fortement dégradé (*République d'Estonie, **Cybersecurity Strategy 2024-2030** ; ENISA*).

Cette politique repose notamment sur une gouvernance nationale clairement identifiée, des mécanismes de coopération entre les secteurs public et privé, le développement des compétences et l'organisation régulière d'exercices de préparation aux crises. Elle s'appuie également sur la participation de spécialistes volontaires réunis au sein de l'unité de cyberdéfense de la Ligue de défense estonienne, qui peut soutenir les autorités en cas de menace majeure (*OTAN-CCDCOE*).

Le pays a également développé le principe d'« ambassade de données ». Cette infrastructure permet de conserver, hors du territoire national mais sous le contrôle juridique de l'État estonien, des copies de données et de systèmes indispensables au fonctionnement de l'administration. L'objectif n'est pas seulement de sauvegarder des informations, mais de permettre la continuité des services publics essentiels en cas d'attaque majeure ou de crise affectant le territoire national (*e-Estonia, **Data Embassy***).

Tallinn accueille par ailleurs le Centre d'excellence de cyberdéfense coopérative de l'OTAN, créé en 2008 à l'initiative de l'Estonie et de plusieurs États alliés. Ce centre contribue à la recherche, à la formation, à l'élaboration de doctrines et à l'organisation d'exercices internationaux de cyberdéfense. Il illustre l'articulation recherchée par l'Estonie entre capacités nationales, coopération européenne et solidarité atlantique (*OTAN-CCDCOE*).

L'expérience estonienne ne peut être transposée mécaniquement à un État de la taille et de la complexité de la France. Elle montre néanmoins qu'une transformation numérique ambitieuse ne peut être durable que si la sécurité, la continuité des services et la souveraineté des données sont intégrées dès la conception des politiques publiques.

Ce que la France peut en retenir : l'expérience estonienne montre que la cybersécurité ne peut demeurer une politique technique ou sectorielle. Elle doit être pleinement intégrée à la stratégie de sécurité nationale, à la continuité de l'État et à la protection des infrastructures essentielles. Elle invite la France à renforcer la gouvernance de la cybersécurité, les exercices de crise, les coopérations entre acteurs publics et privés ainsi que les dispositifs garantissant la continuité des données et des services publics essentiels.

Ce que la Commission retient

Les expériences européennes étudiées ne dessinent pas un modèle unique de politique de sécurité. Elles révèlent cependant une même évolution : les systèmes les plus solides ne reposent plus seulement sur la capacité de l'État à intervenir, mais sur son aptitude à organiser une action continue, coordonnée et anticipatrice. La proximité des forces de sécurité avec les citoyens, l'articulation entre police, justice, collectivités territoriales et acteurs sociaux, la préparation collective aux crises ainsi que l'intégration de la cybersécurité à la stratégie nationale constituent désormais les composantes d'une même politique de protection. La Commission en retient qu'une politique de sécurité moderne doit conjuguer

quatre exigences : une présence publique visible, une gouvernance territoriale décloisonnée, une culture nationale de la prévention et de la résilience, et une maîtrise durable des infrastructures, des compétences et des technologies critiques. La performance ne dépend donc pas uniquement du niveau des moyens engagés, mais de leur coordination, de leur continuité et de leur capacité à produire des résultats concrets pour les citoyens.

Ces enseignements confortent l'orientation générale du présent Cahier : la France doit passer d'une politique principalement fondée sur la réaction à une stratégie de sécurité globale, capable d'anticiper les menaces, de mobiliser l'ensemble de la société et de protéger simultanément les personnes, les territoires, les institutions et les infrastructures numériques essentielles (*Commission européenne ; Europol ; ENISA*).

* * *

LE RAPPORT DE LA COMMISSION

PREMIÈRE PARTIE - Comprendre les nouvelles formes de l'insécurité

Parler de sécurité en 2026 est devenu un exercice délicat. À l'approche des échéances électorales, le sujet nourrit des débats souvent polarisés alors même qu'il demeure l'une des premières préoccupations des Français.

Pourtant, la sécurité ne peut être réduite à un enjeu de circonstance. Elle constitue l'une des missions fondamentales de l'État. Garantir la protection des personnes, des biens et des libertés est le premier devoir de la puissance publique. Cette responsabilité mobilise l'ensemble des acteurs de la sécurité nationale : forces de sécurité intérieure, autorités judiciaires, sécurité civile, armées, collectivités territoriales et, désormais, de nombreux opérateurs publics et privés.

Les travaux de la Commission sont partis d'une interrogation simple : **notre modèle de sécurité est-il encore adapté aux menaces auxquelles la France est aujourd'hui confrontée ?**

Pour y répondre, la Commission a établi un diagnostic fondé sur les données disponibles, confronté les analyses de terrain et comparé l'organisation française à celles de plusieurs partenaires européens. Cette démarche conduit à un double constat.

Le premier concerne l'organisation de notre système de sécurité. La France ne souffre pas seulement d'un manque de moyens. Elle peine surtout à transformer les ressources qu'elle mobilise en une présence visible, coordonnée et efficace sur le terrain. Les procédures demeurent complexes, les responsabilités parfois insuffisamment articulées et une part importante du temps des professionnels reste absorbée par des tâches administratives. L'enjeu n'est donc pas uniquement budgétaire ; il est aussi organisationnel.

Le second constat est plus profond encore : **la nature même de la sécurité a changé.**

Longtemps centrée sur la délinquance de voie publique, le maintien de l'ordre et la lutte contre la criminalité, la politique de sécurité doit désormais répondre à des menaces beaucoup plus diffuses et interdépendantes. Violences du quotidien, terrorisme, criminalité organisée, cybercriminalité, désinformation, ingérences étrangères et attaques contre les infrastructures essentielles participent désormais d'un même environnement stratégique.

Dans ce contexte, la cybersécurité occupe une place nouvelle. Elle ne relève plus du seul domaine technique : elle est devenue une composante de la souveraineté nationale. Les administrations, les entreprises, les collectivités territoriales, les établissements de santé ou d'enseignement, comme les citoyens eux-mêmes, dépendent de systèmes numériques dont la vulnérabilité peut désormais compromettre la continuité des services essentiels.

Les chiffres témoignent de cette évolution. En 2024, 348 000 infractions numériques ont été enregistrées en France, soit une progression de 74 % en cinq ans. En 2025, l'ANSSI a traité 3 586 événements de sécurité touchant principalement les collectivités territoriales, les administrations, les établissements d'enseignement, les hôpitaux et les opérateurs stratégiques.

La sécurité du 21^{ème} siècle ne se joue donc plus uniquement dans l'espace public. Elle se joue également dans le cyberspace, les réseaux numériques, les infrastructures critiques et les systèmes d'information dont dépend le fonctionnement de notre société. Elle suppose d'articuler protection des personnes, résilience des organisations et préservation de notre souveraineté.

C'est à la lumière de cette transformation que la Commission a conduit ses travaux et formulé les analyses et propositions présentées dans ce Cahier.

CHAPITRE 1 - La sécurité commence par l'autorité

La sécurité ne dépend pas uniquement des effectifs de police, des moyens budgétaires ou de l'évolution des statistiques de la délinquance. Elle repose d'abord sur la capacité d'une société à faire respecter des règles communes reconnues comme légitimes. Or les travaux de la Commission montrent que cette capacité s'est progressivement fragilisée.

Au-delà des questions opérationnelles, la France est aujourd'hui confrontée à une crise de l'autorité qui affecte l'ensemble des institutions chargées de faire vivre l'État de droit. Cette évolution ne résulte pas d'un événement isolé mais d'une succession de transformations sociales, culturelles et institutionnelles qui ont profondément modifié le rapport de nos concitoyens à la règle commune.

L'autorité ne se confond ni avec la contrainte ni avec l'autoritarisme. Elle repose sur la reconnaissance de la légitimité des institutions et des règles qui permettent la vie en société. Lorsqu'elle s'affaiblit, c'est l'ensemble du pacte républicain qui devient plus vulnérable.

Une crise de confiance qui fragilise la sécurité

Les auditions conduites par la Commission font apparaître un constat largement partagé : la défiance envers les institutions publiques s'est durablement installée.

Cette défiance touche les représentants de l'État, les élus, les enseignants, les magistrats, les policiers, les professionnels de santé et, plus largement, toutes les autorités chargées d'assurer le respect des règles communes. Elle se traduit par une contestation plus fréquente des décisions publiques, une remise en cause de leur légitimité et une difficulté croissante à faire accepter les règles indispensables à la vie collective.

Le développement des réseaux sociaux, la diffusion instantanée de l'information, la propagation de fausses informations et la polarisation du débat public accentuent ce phénomène. Les autorités traditionnelles sont davantage contestées et le dialogue cède plus facilement la place à l'affrontement.

Pour la Commission, cette crise de confiance constitue désormais un véritable enjeu de sécurité intérieure. Une société qui doute durablement de ses institutions devient plus exposée aux violences, aux manipulations et aux phénomènes de radicalisation.

Une banalisation préoccupante des violences

Cette fragilisation de l'autorité s'observe également dans la multiplication des violences dirigées contre celles et ceux qui incarnent l'autorité publique.

Policiers, gendarmes, sapeurs-pompiers, enseignants, élus locaux ou personnels de santé sont de plus en plus fréquemment confrontés à des insultes, des intimidations ou des agressions physiques.

Au-delà des faits eux-mêmes, cette évolution traduit une remise en cause plus profonde de la règle commune. Elle nourrit un cercle vicieux : plus les représentants de l'autorité sont contestés, plus leur action devient difficile ; plus leur action paraît difficile, plus la confiance des citoyens s'affaiblit.

Rompre cette dynamique constitue une condition essentielle du rétablissement d'une sécurité durable.

La transmission, premier rempart contre l'insécurité

La Commission rappelle que l'autorité ne s'improvise pas : elle se construit et se transmet.

L'école occupe à cet égard une place essentielle. Elle est le premier lieu où l'enfant apprend le respect des règles communes, des autres, de la loi et des valeurs de la République. La transmission des droits, mais aussi des devoirs, constitue une dimension fondamentale de la politique de sécurité.

Cette responsabilité ne relève toutefois pas des seuls enseignants.

Les auditions rappellent avec force que la famille demeure le premier lieu de socialisation. Les parents sont les premiers transmetteurs de l'autorité, du sens des responsabilités et du respect des règles. Lorsque cette transmission devient plus difficile, les institutions sont conduites à compenser des fragilités qui dépassent leur mission première.

La Commission estime dès lors que les politiques publiques doivent mieux accompagner les familles dans l'exercice de leurs responsabilités éducatives. Le soutien à la parentalité, le dialogue avec les établissements scolaires et les actions de prévention participent pleinement de la politique de sécurité.

Restaurer une culture de la responsabilité

Les travaux de la Commission conduisent à une conviction simple : aucune politique de sécurité ne peut produire durablement ses effets sans une restauration progressive de la responsabilité individuelle et collective.

Cette responsabilité incombe naturellement aux institutions publiques, qui doivent être exemplaires, lisibles et efficaces. Mais elle concerne également les familles, les entreprises, les associations et l'ensemble des citoyens.

Restaurer l'autorité ne consiste pas à multiplier les contraintes. Il s'agit de redonner toute sa place à la règle commune, de réaffirmer les principes de la République et de recréer les conditions d'une confiance durable entre les citoyens et leurs institutions.

La sécurité repose certes sur des moyens humains, des équipements performants et une organisation efficace. Mais elle repose tout autant sur une société capable de reconnaître la légitimité de ses institutions et d'accepter les règles qui rendent possible la vie en commun.

La Commission considère ainsi que la restauration de l'autorité constitue l'un des principaux défis de la politique de sécurité. Elle conditionne l'efficacité des forces de sécurité, de l'institution judiciaire et, plus largement, de l'ensemble des services publics chargés de faire vivre l'État de droit.

CHAPITRE 2 - Les forces de sécurité : des moyens importants, une efficacité à renforcer

La France dispose de forces de sécurité parmi les plus professionnelles d'Europe. Police nationale, Gendarmerie nationale, polices municipales, douanes, sécurité civile et, dans certaines circonstances, forces armées concourent quotidiennement à la protection des personnes, des biens et des institutions de la République.

Depuis plusieurs années, les moyens humains, budgétaires et matériels ont été significativement renforcés. Les différentes lois de programmation ont permis de moderniser les équipements, d'accroître les effectifs et d'investir dans les technologies numériques.

Pourtant, les auditions conduites par la Commission font apparaître un paradoxe largement partagé : malgré cet effort, les Français continuent d'exprimer un fort sentiment d'insécurité et les professionnels eux-mêmes estiment ne pas toujours disposer des conditions nécessaires pour exercer pleinement leurs missions.

La Commission en tire une conclusion simple : la question n'est plus seulement celle des moyens. Elle est devenue celle de leur efficacité.

Une organisation devenue complexe

Le système français repose sur une pluralité d'acteurs dont les compétences sont complémentaires.

Police nationale, Gendarmerie nationale, polices municipales, douanes, sécurité civile, justice, services de renseignement et collectivités territoriales interviennent selon des responsabilités clairement définies.

Cette diversité constitue une force. Elle permet une couverture complète du territoire et une spécialisation des missions.

Elle suppose cependant une coordination permanente.

Les auditions montrent que la multiplication des procédures, des niveaux de décision et des acteurs peut parfois ralentir l'action publique, compliquer les échanges d'information et réduire la lisibilité de l'organisation pour les citoyens comme pour les professionnels.

L'enjeu n'est donc pas de modifier l'architecture générale du système, mais de mieux articuler les responsabilités de chacun.

Redonner du temps au terrain

Le constat revient dans l'ensemble des auditions : une part importante du temps des policiers et des gendarmes est aujourd'hui absorbée par les procédures administratives.

Rédaction des procédures judiciaires, formalités administratives, gardes statatiques, extractions ou missions périphériques limitent le temps consacré à la présence opérationnelle.

Or cette présence constitue l'un des premiers facteurs de confiance des citoyens.

Voir des policiers et des gendarmes sur le terrain contribue à prévenir les infractions, rassurer la population, recueillir le renseignement de proximité et renforcer le lien entre les forces de sécurité et les habitants.

Pour la Commission, restaurer cette présence constitue une priorité.

Préserver l'engagement des femmes et des hommes

La qualité d'une politique de sécurité dépend d'abord des femmes et des hommes qui la mettent en œuvre.

Les professionnels entendus par la Commission expriment un attachement profond à leur mission de service public. Ils évoquent cependant une accumulation de contraintes : complexité des procédures, pression opérationnelle, horaires difficiles, violences croissantes contre les représentants de l'autorité et sentiment que les résultats de leur engagement demeurent parfois insuffisamment visibles.

Préserver l'attractivité des métiers de la sécurité constitue dès lors un enjeu stratégique.

La fidélisation des personnels passe autant par l'amélioration des conditions d'exercice que par la reconnaissance de leur engagement.

Adapter les compétences aux nouvelles menaces

Les missions des forces de sécurité ont profondément évolué.

Aux missions traditionnelles de maintien de l'ordre et de lutte contre la délinquance se sont ajoutées la lutte contre le terrorisme, la criminalité organisée, les violences intrafamiliales, la cybercriminalité, les fraudes numériques ou encore la protection des infrastructures critiques.

Cette évolution impose une adaptation permanente des compétences.

La Commission estime que la formation continue doit devenir un véritable levier de transformation. Elle recommande également de développer des formations communes entre policiers, gendarmes, magistrats et spécialistes de la cybersécurité afin de renforcer la coopération entre les différents acteurs de la chaîne de sécurité.

Faire de l'efficacité le premier objectif

Au terme de ses travaux, la Commission considère que la sécurité gagnera moins à une multiplication des réformes institutionnelles qu'à une amélioration de l'organisation existante.

Simplifier les procédures, renforcer la coordination entre les services, recentrer les forces de sécurité sur leurs missions opérationnelles, moderniser les outils de travail et développer une culture de l'évaluation constituent les principaux leviers d'une action publique plus efficace.

La sécurité ne se mesure pas uniquement au nombre d'effectifs ou au montant des crédits engagés. Elle se mesure à la capacité de l'État à protéger concrètement les citoyens, à intervenir rapidement lorsque cela est nécessaire et à garantir une présence visible de la puissance publique sur l'ensemble du territoire.

CHAPITRE 3 - Justice : restaurer l'efficacité de la chaîne pénale

La sécurité ne s'arrête pas à l'interpellation d'un auteur d'infraction. Elle ne produit pleinement ses effets que lorsque l'action des forces de sécurité est relayée par une réponse judiciaire rapide, compréhensible et effectivement exécutée.

Les travaux de la Commission montrent que police, gendarmerie, justice et administration pénitentiaire ne constituent pas des institutions indépendantes les unes des autres. Elles forment les différents maillons d'une même chaîne au service de l'État de droit. Lorsque l'un d'eux se fragilise, c'est l'ensemble de la politique de sécurité qui perd en efficacité et en crédibilité.

La Commission en tire une conviction : restaurer la confiance dans la sécurité suppose également de restaurer la confiance dans la justice.

Une chaîne pénale qui doit gagner en fluidité

La justice française est confrontée à une augmentation constante du nombre de procédures, à une diversification des contentieux et à une exigence croissante de garanties procédurales.

Cette évolution constitue un progrès pour la protection des libertés individuelles. Elle s'accompagne toutefois d'une complexité accrue des procédures et d'un allongement des délais de traitement.

Les auditions conduites par la Commission montrent que cette situation mobilise une part importante des ressources des juridictions comme des services enquêteurs. Les policiers et les gendarmes consacrent un temps considérable à la rédaction des procédures, tandis que les magistrats doivent traiter un volume croissant d'affaires dans des délais souvent contraints.

L'enjeu n'est pas de remettre en cause les garanties de l'État de droit, mais de rendre la chaîne pénale plus fluide afin qu'elle puisse répondre plus rapidement aux attentes des citoyens.

Une justice plus rapide pour une justice plus crédible

Les citoyens attendent qu'une infraction donne lieu à une réponse compréhensible dans un délai raisonnable. Les victimes souhaitent être reconnues et protégées ; les forces de sécurité attendent que les procédures auxquelles elles consacrent un investissement important trouvent une traduction judiciaire effective.

Or les délais de traitement peuvent parfois apparaître difficilement compréhensibles. Ce décalage entre le temps judiciaire et le temps vécu nourrit un sentiment d'incompréhension qui fragilise la confiance dans l'institution.

Pour la Commission, la rapidité de la réponse judiciaire constitue désormais un véritable enjeu de sécurité. Une justice rendue trop tard perd une partie de son efficacité, même lorsque la décision est juridiquement fondée.

Donner toute sa force à l'exécution des peines

La crédibilité de la justice ne dépend pas uniquement des décisions prononcées. Elle repose également sur leur exécution effective.

Lorsque les peines apparaissent insuffisamment exécutées ou difficilement lisibles, elles alimentent le sentiment d'un écart entre les infractions constatées et leurs conséquences.

La Commission souligne que l'objectif n'est pas d'alourdir systématiquement les sanctions, mais de garantir que les décisions de justice soient appliquées dans des conditions compatibles avec leur finalité, tant pour les victimes que pour les personnes condamnées.

L'exécution des peines constitue ainsi l'un des fondements de l'autorité de la justice.

Moderniser la politique pénitentiaire

La réflexion sur la chaîne pénale ne peut ignorer la situation des établissements pénitentiaires.

Les auditions de la Commission mettent en évidence les effets de la surpopulation carcérale, les difficultés rencontrées par les personnels et les enjeux liés à la préparation de la réinsertion.

La prison demeure un instrument indispensable pour protéger la société contre les auteurs des infractions les plus graves. Elle ne peut cependant constituer l'unique réponse de la politique pénale.

La Commission estime nécessaire de poursuivre les efforts de modernisation du parc pénitentiaire, d'améliorer les conditions d'exercice des personnels et de renforcer les dispositifs favorisant la prévention de la récidive et la préparation du retour à la vie sociale.

Renforcer la coopération entre tous les acteurs

Les auditions montrent qu'il serait artificiel d'opposer police, gendarmerie et justice.

Toutes poursuivent un même objectif : garantir l'application de la loi et protéger les citoyens.

Les difficultés constatées relèvent moins d'une opposition entre institutions que d'une articulation parfois insuffisante entre leurs missions respectives.

La Commission considère qu'une meilleure connaissance mutuelle des contraintes professionnelles, le développement de formations communes et une simplification des procédures permettront de renforcer l'efficacité collective de la chaîne pénale.

Restaurer la confiance dans la justice

Au terme de ses travaux, la Commission considère que la sécurité et la justice ne peuvent être dissociées.

Une police efficace sans réponse judiciaire lisible perd progressivement en crédibilité. Une justice de qualité qui intervient trop tard peine à produire tous ses effets. Une politique pénitentiaire insuffisamment adaptée fragilise également l'ensemble du dispositif.

L'amélioration de la chaîne pénale repose moins sur une succession de réformes institutionnelles que sur une meilleure articulation entre les acteurs, une simplification des procédures, une réduction des délais et une exécution plus effective des décisions de justice.

La confiance des citoyens dépend de la capacité de chaque maillon à remplir pleinement sa mission. Restaurer l'efficacité de la chaîne pénale, c'est renforcer simultanément l'autorité de la justice, l'action des forces de sécurité et la crédibilité de l'État de droit.

* * *

Conclusion de la première partie

Restaurer les fondements de la sécurité

Au terme de cette première partie, la Commission retient un enseignement majeur : la sécurité ne dépend pas d'un seul acteur ni d'une seule institution. Elle repose sur la solidité de l'ensemble de la chaîne qui relie l'autorité de l'État, l'action des forces de sécurité et l'efficacité de la justice.

Les auditions montrent que la France ne manque ni de compétences, ni d'engagement, ni de moyens. Les policiers, les gendarmes, les magistrats et les personnels pénitentiaires accomplissent leurs missions avec professionnalisme dans un contexte souvent exigeant. Les difficultés tiennent davantage à la complexité des organisations, à l'allongement des procédures, à une articulation parfois insuffisante entre les acteurs et à une crise plus profonde de la confiance dans les institutions.

La Commission en tire une conviction simple : restaurer la sécurité suppose de restaurer simultanément l'autorité, l'efficacité opérationnelle et la crédibilité de la chaîne pénale. Chacun de ces leviers est indispensable ; aucun ne peut produire pleinement ses effets sans les autres.

Mais ce diagnostic, aussi essentiel soit-il, ne suffit plus à rendre compte des défis auxquels notre pays est confronté.

La sécurité du 21^{ème} siècle ne se joue plus seulement dans l'espace public. Elle se construit également en amont des violences, dans l'éducation, la prévention, la protection des infrastructures critiques, la maîtrise des risques numériques et la capacité de la Nation à faire face aux crises.

C'est pourquoi la Commission invite à dépasser une conception exclusivement régalienne de la sécurité pour promouvoir une approche plus globale, associant l'ensemble des acteurs publics et privés autour d'une même ambition : protéger durablement les Français et renforcer la résilience de la Nation.

Cette évolution constitue l'objet de la deuxième partie de ce Cahier. Elle montre que la sécurité n'est plus seulement une politique de protection ; elle est devenue une politique d'anticipation, de prévention et de souveraineté.

* * *

DEUXIÈME PARTIE - La sécurité du 21^{ème} siècle : vers une approche globale

Pendant longtemps, la sécurité en France a été pensée autour de missions clairement identifiées : lutter contre la délinquance, maintenir l'ordre public, protéger les personnes et les biens, prévenir le terrorisme. Les forces de sécurité intérieure, la justice et les services de renseignement constituaient les principaux piliers de cette politique publique.

Ces missions demeurent naturellement essentielles. Elles ne suffisent cependant plus à répondre aux défis auxquels notre pays est désormais confronté.

Les travaux de la Commission montrent que la nature même des menaces s'est profondément transformée. Aux violences du quotidien s'ajoutent aujourd'hui le terrorisme, la criminalité organisée, les ingérences étrangères, les campagnes de désinformation et les attaques contre les infrastructures numériques. Les frontières entre sécurité intérieure, justice, renseignement, défense et cybersécurité deviennent de plus en plus perméables.

Dans ce nouvel environnement, la distinction entre sécurité physique et sécurité numérique tend progressivement à disparaître. La protection des personnes ne peut plus être dissociée de celle des données, des réseaux, des administrations, des entreprises ou des infrastructures essentielles dont dépend le fonctionnement de la Nation.

La cybersécurité n'est plus une question réservée aux spécialistes de l'informatique. Elle est devenue un enjeu majeur de souveraineté nationale. Elle conditionne la continuité des services publics, la compétitivité de notre économie, la protection des infrastructures critiques et, plus largement, la confiance des citoyens dans les institutions.

Cette évolution est désormais pleinement reconnue par la **Stratégie nationale de cybersécurité 2026-2030**, qui qualifie le cyberspace de « théâtre de puissance » et fixe pour ambition de faire de la France une puissance souveraine dans le domaine numérique. Les attaques informatiques ne constituent plus un risque périphérique : elles sont devenues une menace susceptible d'affecter directement le fonctionnement de l'État, l'économie et les services essentiels de la Nation.

Les crises récentes illustrent cette mutation.

La crise sanitaire a accéléré la numérisation des organisations et le recours massif au télétravail. Si cette évolution a permis d'assurer la continuité de nombreuses activités, elle a également considérablement accru la surface d'exposition aux cyberattaques. Le déploiement rapide d'accès distants, la multiplication des postes de travail nomades et l'ouverture de nombreux services sur Internet ont créé de nouvelles vulnérabilités, aujourd'hui largement exploitées par les organisations criminelles.

Dans le même temps, les conflits internationaux ont profondément renouvelé la perception du risque cyber. La guerre en Ukraine a montré que les opérations militaires s'accompagnent désormais d'attaques informatiques, de campagnes de

désinformation, de tentatives d'espionnage et d'actions visant à déstabiliser les infrastructures critiques. Les États ne sont plus les seuls acteurs : groupes criminels, hacktivistes et organisations liées à des puissances étrangères interviennent désormais dans un espace où les frontières entre criminalité, influence et confrontation stratégique deviennent de plus en plus floues.

Le diagnostic établi par la Commission est sans ambiguïté.

En 2024, **348 000 infractions numériques** ont été enregistrées en France, soit une augmentation de **74 % en cinq ans**. En 2025, l'ANSSI a traité **3 586 événements de sécurité**, touchant principalement les ministères, les collectivités territoriales, les établissements d'enseignement, les structures de santé et les opérateurs de télécommunications. Ces chiffres traduisent une menace devenue permanente, qui affecte désormais l'ensemble des activités de la Nation.

La nature même de cette menace a également changé. La figure du pirate informatique isolé laisse progressivement place à une véritable économie criminelle organisée. Certains groupes développent des outils d'attaque, d'autres commercialisent des accès à des systèmes déjà compromis, tandis que d'autres encore conduisent les opérations d'extorsion ou de sabotage. L'intelligence artificielle, les cryptoactifs et les places de marché clandestines renforcent encore leurs capacités d'action. La cybercriminalité est devenue une activité industrielle.

Face à cette évolution, la Commission considère que la sécurité doit désormais être pensée autour de trois exigences complémentaires.

La première consiste à garantir la protection des personnes et des biens, qui demeure la mission fondamentale des forces de sécurité intérieure.

La deuxième vise à prévenir, détecter et neutraliser les menaces numériques avant qu'elles ne compromettent le fonctionnement des services essentiels.

La troisième repose sur le renforcement de la résilience de l'État, c'est-à-dire sa capacité à assurer la continuité de ses missions, à protéger ses infrastructures critiques et à préserver sa souveraineté numérique.

L'enjeu dépasse désormais la seule sécurité intérieure. Il concerne le fonctionnement des administrations, la protection des collectivités territoriales, la sécurité des établissements de santé, la continuité des réseaux de transport, la stabilité du système financier, la protection des données personnelles et, plus largement, la confiance dans les institutions démocratiques.

La sécurité du 21^{ème} siècle se joue désormais autant dans les rues que dans les réseaux. Elle suppose une approche globale associant les forces de sécurité, la justice, le renseignement, les collectivités territoriales, les entreprises, les établissements publics, le monde académique et les citoyens.

Cette mutation constitue l'un des principaux défis auxquels la France est aujourd'hui confrontée. Elle appelle une réponse qui ne soit plus seulement policière ou judiciaire, mais également technologique, industrielle, éducative et stratégique.

Les chapitres qui suivent analysent cette transformation en s'appuyant largement sur les travaux consacrés à la cybersécurité. Ils montrent que la protection du cyberspace est désormais l'une des conditions de la souveraineté nationale, de la continuité de l'action publique et de la résilience de notre pays.

CHAPITRE 4 - Comprendre la révolution cyber

Pourquoi le cyber change la nature même de la sécurité

Pendant longtemps, la sécurité a été conçue comme la protection des personnes, des biens et du territoire national. Cette mission demeure au cœur des responsabilités de l'État. Elle ne suffit cependant plus à répondre aux défis auxquels la France est aujourd'hui confrontée.

La transformation numérique a profondément modifié le fonctionnement de notre société. Les administrations, les entreprises, les collectivités territoriales, les établissements de santé, les infrastructures de transport, les réseaux énergétiques, les établissements scolaires et les citoyens dépendent désormais quotidiennement de systèmes d'information interconnectés. Cette numérisation constitue un puissant levier de modernisation, d'efficacité et d'innovation. Elle crée également une dépendance nouvelle à des infrastructures numériques dont la vulnérabilité peut avoir des conséquences majeures.

La sécurité est ainsi entrée dans une nouvelle dimension.

Elle ne se joue plus uniquement dans l'espace public. Elle se joue également dans les réseaux numériques, les centres de données, les systèmes industriels, les plateformes numériques et les infrastructures essentielles au fonctionnement de la Nation.

Le cyberspace est devenu un espace de confrontation à part entière.

La protection des données, des réseaux et des systèmes d'information ne relève plus uniquement des spécialistes de l'informatique. Elle conditionne désormais la continuité des services publics, la compétitivité économique, le fonctionnement des institutions démocratiques et, plus largement, l'exercice de la souveraineté nationale.

Les travaux de la Commission conduisent à une conviction simple : la cybersécurité est désormais l'une des composantes essentielles de la sécurité nationale.

Une mutation profonde des menaces

La nature des menaces numériques a profondément évolué au cours des dernières années.

La crise sanitaire a constitué un accélérateur majeur. Afin d'assurer la continuité des activités, les organisations publiques comme privées ont généralisé le télétravail dans des délais très courts. Elles ont multiplié les accès distants, ouvert de nouveaux services accessibles depuis Internet et déployé massivement des postes de travail nomades. Cette transformation, indispensable sur le plan

économique et social, a également accru les vulnérabilités des systèmes d'information.

Parallèlement, les conflits internationaux ont profondément renouvelé la perception du risque cyber.

La guerre en Ukraine a montré que les opérations militaires s'accompagnent désormais d'attaques informatiques, d'opérations d'espionnage, de campagnes de désinformation et de tentatives de déstabilisation des infrastructures essentielles. Les actions menées dans le cyberspace ne constituent plus un simple soutien aux opérations militaires : elles participent pleinement de la confrontation stratégique.

Les États ne sont d'ailleurs plus les seuls acteurs.

Groupes criminels, hacktivistes, organisations liées à des puissances étrangères et réseaux spécialisés interviennent simultanément dans un environnement où les frontières entre criminalité, influence, espionnage et conflictualité deviennent de plus en plus difficiles à distinguer.

La sécurité ne peut donc plus être pensée selon une séparation stricte entre monde physique et monde numérique. Les deux dimensions sont désormais étroitement liées.

Le risque cyber : un risque systémique

Le risque cyber peut être défini comme le risque qu'une atteinte à un système d'information compromette la confidentialité, l'intégrité, la disponibilité ou l'authenticité des données et des services numériques.

À la différence de nombreux risques opérationnels traditionnels, il présente plusieurs caractéristiques particulières.

D'abord, les attaques peuvent se propager extrêmement rapidement et affecter simultanément un grand nombre d'organisations.

Ensuite, elles sont le plus souvent intentionnelles et s'adaptent en permanence aux dispositifs de protection mis en œuvre.

Enfin, leurs conséquences dépassent fréquemment l'organisation directement visée. Une attaque contre un prestataire informatique, un fournisseur de logiciels ou un opérateur de services peut affecter des centaines, voire des milliers d'organisations en cascade.

Le risque cyber devient ainsi un risque systémique.

Sa mesure demeure complexe. De nombreuses organisations hésitent encore à déclarer les incidents dont elles sont victimes, par crainte d'effets négatifs sur leur réputation, leur activité ou leur valeur économique.

Les conséquences dépassent largement le coût immédiat des attaques. Elles comprennent également les interruptions d'activité, la perte de données, l'atteinte à l'image, les coûts de remise en état des systèmes d'information, les pertes de

propriété intellectuelle et la dégradation durable de la confiance des clients, des partenaires ou des usagers.

Une cybercriminalité devenue industrielle

L'image du pirate informatique agissant seul appartient désormais largement au passé.

Les travaux de la Commission montrent que la cybercriminalité s'est progressivement organisée autour d'un véritable modèle économique.

Certains groupes développent des logiciels malveillants, d'autres identifient des vulnérabilités ou compromettent des systèmes d'information. D'autres encore commercialisent des accès déjà piratés, proposent des services d'attaque « clés en main » ou conduisent les opérations d'extorsion.

Les rançongiciels, les campagnes d'hameçonnage, les attaques contre les chaînes d'approvisionnement numériques, les opérations d'espionnage économique ou les fraudes utilisant l'ingénierie sociale constituent désormais des modes opératoires courants.

L'intelligence artificielle, les cryptoactifs et les places de marché clandestines renforcent encore les capacités de ces organisations criminelles.

La cybercriminalité fonctionne désormais selon une logique industrielle, internationale et fortement spécialisée.

Les administrations, les collectivités territoriales, les établissements de santé, les entreprises industrielles, les opérateurs de transport, les banques, les universités et les PME figurent aujourd'hui parmi les cibles privilégiées.

Un enjeu économique majeur

Les conséquences économiques de cette évolution sont considérables.

Une cyberattaque peut interrompre durablement l'activité d'une entreprise, désorganiser un établissement hospitalier, bloquer une collectivité territoriale ou perturber le fonctionnement d'une administration.

Au-delà des coûts directs, les attaques fragilisent la confiance indispensable au fonctionnement des échanges économiques.

Le numérique constitue aujourd'hui l'infrastructure invisible de l'économie contemporaine. Toute atteinte à cette infrastructure produit des effets bien au-delà des seuls systèmes informatiques.

Pour certaines organisations, une cyberattaque majeure peut remettre en cause leur pérennité.

La cybersécurité devient ainsi un enjeu de compétitivité autant que de protection.

Un enjeu de souveraineté nationale

Cette évolution dépasse désormais le seul champ économique.

Les infrastructures numériques soutiennent le fonctionnement quotidien de l'État, des collectivités territoriales, des réseaux énergétiques, des transports, du système de santé, des communications, des établissements financiers et des services publics essentiels.

Une attaque contre ces infrastructures peut provoquer des conséquences comparables à celles d'une crise majeure.

La protection du cyberspace participe donc directement de la continuité de l'État.

La cybersécurité ne constitue plus une politique technique parmi d'autres. Elle devient l'une des expressions de la souveraineté nationale.

Protéger les données, les réseaux, les infrastructures critiques et les systèmes d'information revient désormais à protéger la capacité même de la Nation à fonctionner en toute circonstance.

Cette évolution conduit à repenser la sécurité dans son ensemble.

Elle suppose de dépasser une approche exclusivement réactive pour développer une véritable stratégie de prévention, d'anticipation et de résilience.

C'est précisément l'objet du chapitre suivant, consacré à l'organisation de la réponse française face à la cybermenace, à la stratégie nationale de cybersécurité et aux moyens mobilisés pour renforcer durablement la résilience de notre pays.

CHAPITRE 5 - L'État face à la cybermenace

Une organisation progressivement structurée

La montée en puissance des cybermenaces a profondément transformé l'action de l'État. Longtemps considérée comme une problématique principalement technique, la cybersécurité constitue désormais une composante essentielle de la sécurité nationale. La protection des administrations, des collectivités territoriales, des entreprises stratégiques et des infrastructures critiques conditionne aujourd'hui la continuité des services publics, le fonctionnement de l'économie et l'exercice de la souveraineté.

Cette évolution a conduit les pouvoirs publics à bâtir progressivement une véritable stratégie nationale, fondée sur une gouvernance dédiée, des capacités opérationnelles renforcées et une coopération croissante entre les acteurs publics et privés. La France dispose aujourd'hui d'un dispositif reconnu, qui doit toutefois continuer à évoluer pour répondre à des menaces toujours plus nombreuses, plus complexes et plus rapides.

Une stratégie nationale désormais affirmée

Au cours des dernières années, la cybersécurité s'est progressivement imposée comme une priorité stratégique de l'action publique.

La stratégie nationale de cybersécurité poursuit plusieurs objectifs complémentaires : protéger les administrations et les services publics, renforcer la sécurité des opérateurs d'importance vitale, développer une filière industrielle française et européenne, accroître les capacités nationales de détection et de réponse aux incidents, et diffuser une véritable culture de cybersécurité auprès des administrations, des entreprises et des citoyens.

Cette stratégie traduit une évolution importante de la doctrine française. La cybersécurité n'est plus envisagée comme une simple question informatique. Elle participe désormais pleinement de la souveraineté nationale, de la compétitivité économique et de la résilience de la Nation.

Une gouvernance progressivement structurée

Cette montée en puissance s'est accompagnée d'une structuration progressive des responsabilités.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) constitue aujourd'hui l'autorité de référence en matière de prévention, de détection et de réponse aux incidents affectant les administrations et les opérateurs stratégiques. Son rôle dépasse désormais l'assistance technique : elle contribue à l'élaboration de la doctrine nationale, accompagne les acteurs publics et privés et participe au renforcement de la résilience du pays.

À ses côtés interviennent plusieurs acteurs spécialisés.

Le Commandement du ministère de l'Intérieur dans le cyberespace (COMCYBER-MI) coordonne les capacités cyber du ministère de l'Intérieur. Les armées disposent de leurs propres capacités de cyberdéfense. Les services de renseignement participent à la détection des menaces, tandis que les autorités judiciaires assurent la poursuite des infractions numériques.

Les collectivités territoriales, les opérateurs d'importance vitale et les entreprises exploitant des infrastructures essentielles occupent également une place croissante dans ce dispositif.

Cette organisation reflète une conviction désormais largement partagée : la cybersécurité ne relève plus d'un acteur unique mais d'une responsabilité collective mobilisant l'ensemble des administrations concernées.

Une coopération devenue indispensable

La majorité des infrastructures numériques critiques est aujourd'hui exploitée par des acteurs privés.

Les réseaux de télécommunications, les établissements financiers, les opérateurs énergétiques, les entreprises de transport, les plateformes numériques ou encore

les établissements de santé assurent des fonctions indispensables au fonctionnement du pays.

La protection de ces infrastructures ne peut donc reposer sur l'État seul.

Les travaux de la Commission montrent que la résilience nationale dépend désormais de la qualité de la coopération entre les administrations, les entreprises et les opérateurs stratégiques. Le partage d'informations sur les incidents, l'harmonisation des exigences de sécurité, les exercices communs de gestion de crise et la diffusion des bonnes pratiques constituent désormais des leviers essentiels de la politique nationale de cybersécurité.

Cette coopération apparaît d'autant plus nécessaire que les attaques ciblent désormais des chaînes complètes de sous-traitance, où la vulnérabilité d'un acteur peut compromettre l'ensemble d'un écosystème.

Des moyens renforcés mais des fragilités persistantes

Les investissements consacrés à la cybersécurité ont connu une progression importante.

Les effectifs spécialisés augmentent, les capacités de surveillance se modernisent et les exercices de gestion de crise se multiplient. Cette dynamique témoigne de la prise de conscience des pouvoirs publics.

Les auditions conduites par la Commission mettent toutefois en évidence plusieurs fragilités.

La première concerne la pénurie de compétences. Les administrations, les collectivités territoriales et les entreprises rencontrent des difficultés croissantes pour recruter des spécialistes capables de faire face à des attaques toujours plus sophistiquées.

La deuxième réside dans l'hétérogénéité du niveau de protection des territoires. Les collectivités territoriales, en particulier les communes de taille moyenne ou modeste, disposent de moyens humains et financiers très variables alors qu'elles constituent désormais des cibles privilégiées des cybercriminels.

Enfin, la dépendance à certaines technologies étrangères demeure un enjeu majeur de souveraineté. Si la France dispose d'un écosystème reconnu dans plusieurs domaines, elle reste tributaire de solutions numériques développées hors d'Europe pour certaines fonctions essentielles.

Ces fragilités invitent à poursuivre les efforts engagés afin de renforcer durablement la résilience du pays.

Les défis des prochaines années

Au terme de ses travaux, la Commission estime que les progrès accomplis sont réels.

La France dispose désormais d'une stratégie nationale clairement identifiée, d'institutions reconnues et d'une expertise de haut niveau. Elle bénéficie

également d'un cadre européen de plus en plus structurant, qui renforce la coopération entre les États membres.

Pour autant, les menaces évoluent plus rapidement que les organisations.

La multiplication des attaques, la sophistication croissante des groupes criminels, la concurrence internationale pour les compétences, les dépendances technologiques et la nécessité d'accompagner l'ensemble des collectivités territoriales imposent de poursuivre les efforts engagés.

La cybersécurité ne peut plus être conçue comme une succession de réponses à des crises ponctuelles. Elle doit s'inscrire dans une politique publique de long terme, fondée sur l'anticipation, l'innovation, la coopération et la résilience.

À ce titre, elle constitue désormais l'un des piliers de la sécurité nationale et l'une des conditions essentielles de la souveraineté française dans le monde numérique.

CHAPITRE 6 - Former une Nation cyber-résiliente

Le facteur humain, premier rempart contre la cybermenace

Les travaux de la Commission conduisent à un constat simple : la cybersécurité ne repose pas uniquement sur la qualité des technologies, des logiciels ou des infrastructures. Elle dépend tout autant de la capacité des femmes et des hommes à adopter les comportements permettant de prévenir, détecter et signaler les incidents.

Dans un environnement où les cyberattaques exploitent aussi bien les failles techniques que les erreurs humaines, le facteur humain devient l'un des principaux déterminants de la sécurité nationale. Un mot de passe insuffisamment protégé, un courriel frauduleux ouvert par inadvertance ou une mauvaise manipulation peuvent compromettre le fonctionnement d'une administration, d'une entreprise ou d'un service public.

La Commission considère que la cybersécurité ne peut plus être réservée aux seuls spécialistes. Elle doit progressivement devenir une culture commune, partagée par l'ensemble des administrations, des collectivités territoriales, des entreprises et des citoyens.

Faire de la formation une priorité stratégique

Cette évolution conduit naturellement à placer la formation au cœur de la politique nationale de cybersécurité.

La France a engagé un effort important dans ce domaine. Le plan stratégique de l'ANSSI, la Stratégie nationale de cybersécurité 2026-2030 ainsi que la création du Centre national de formation cyber du COMCYBER-MI témoignent d'une volonté de développer durablement les compétences nécessaires pour faire face aux nouvelles menaces.

Ces initiatives traduisent une évolution majeure : la formation n'est plus un simple accompagnement des politiques publiques. Elle constitue désormais l'une des conditions de leur efficacité.

Former davantage de spécialistes demeure indispensable. Mais la résilience nationale suppose également que chaque agent public, chaque élu, chaque responsable d'organisation maîtrise les réflexes élémentaires de sécurité numérique dans l'exercice quotidien de ses fonctions.

Développer une véritable culture de cybersécurité

La Commission souligne que la première ligne de défense reste constituée par les utilisateurs eux-mêmes.

La protection des identifiants, l'utilisation d'une authentification renforcée, la capacité à reconnaître une tentative d'hameçonnage, la sauvegarde régulière des données ou encore le signalement rapide d'un incident relèvent désormais des compétences professionnelles de base.

Ces pratiques, parfois qualifiées d'« hygiène numérique », ne constituent plus de simples recommandations techniques. Elles participent pleinement de la sécurité des organisations.

Développer une véritable culture de cybersécurité revient ainsi à diffuser des comportements adaptés bien au-delà des seuls services informatiques. Dans un environnement numérique largement interconnecté, chaque utilisateur contribue, à son niveau, à la protection de l'ensemble du système.

Adapter les compétences aux responsabilités

Tous les acteurs ne sont toutefois pas confrontés aux mêmes risques.

Les travaux de la Commission montrent qu'une politique de formation efficace suppose de différencier les parcours selon les responsabilités exercées.

Un premier niveau concerne l'ensemble des agents publics, appelés à maîtriser les principes fondamentaux de la sécurité numérique.

Un deuxième niveau s'adresse aux personnels exerçant des fonctions particulièrement exposées ou manipulant des données sensibles.

Enfin, un troisième niveau doit permettre de former des spécialistes capables d'assurer les missions de prévention, de détection, d'analyse et de réponse aux incidents.

Cette gradation des compétences permet de mieux répondre à la diversité des besoins tout en structurant de véritables parcours professionnels dans les métiers de la cybersécurité.

Accompagner durablement les territoires

Les collectivités territoriales occupent désormais une place essentielle dans la résilience numérique du pays.

La dématérialisation des services publics locaux, le développement des systèmes d'information et l'interconnexion croissante des réseaux ont considérablement accru leur exposition aux cyberattaques.

Or les moyens disponibles restent très inégaux selon la taille des collectivités.

Les auditions conduites par la Commission montrent que de nombreuses communes, établissements publics ou structures hospitalières disposent de ressources limitées pour recruter des spécialistes ou organiser des dispositifs de protection adaptés.

La Commission estime qu'un accompagnement spécifique doit être poursuivi afin de développer la formation des agents, favoriser le partage d'expériences, mutualiser certaines compétences et organiser régulièrement des exercices de gestion de crise.

La résilience nationale dépend en effet directement de la capacité des territoires à maintenir la continuité de leurs services essentiels face aux incidents numériques.

Sensibiliser l'ensemble de la société

La cybersécurité dépasse largement le seul champ des administrations publiques.

Les entreprises, notamment les PME, figurent aujourd'hui parmi les principales cibles des organisations criminelles, tandis que les citoyens sont quotidiennement confrontés aux tentatives d'escroquerie, aux fraudes bancaires, aux vols de données ou aux usurpations d'identité.

Face à cette évolution, la Commission considère que la sensibilisation doit devenir une politique publique permanente.

Campagnes nationales d'information, plateformes d'assistance, outils pédagogiques, actions de prévention et exercices de sensibilisation doivent contribuer à développer une véritable culture du risque numérique au sein de l'ensemble de la société.

La sécurité du cyberspace ne peut reposer uniquement sur les administrations spécialisées. Elle suppose une vigilance collective et une responsabilité partagée.

Les compétences, nouvel enjeu de souveraineté

Au terme de ses travaux, la Commission retient que les compétences constituent désormais l'une des ressources stratégiques de la souveraineté numérique.

Les infrastructures les plus performantes demeurent vulnérables si les organisations ne disposent pas des femmes et des hommes capables de les concevoir, de les administrer et de les protéger.

La souveraineté numérique se construit donc autant dans les établissements d'enseignement, les centres de formation, les administrations et les entreprises que dans les centres opérationnels de cybersécurité.

Former une Nation cyber-résiliente ne relève plus d'une politique sectorielle. Il s'agit désormais d'un investissement stratégique au service de la sécurité nationale, de la compétitivité économique et de la continuité de l'État.

Ainsi, la résilience numérique de la France dépendra moins de sa seule capacité à acquérir des technologies performantes que de sa capacité à développer durablement les compétences nécessaires pour les maîtriser et les faire évoluer.

Conclusion de la deuxième partie

De la protection à la résilience

Au terme de cette deuxième partie, la Commission retient un enseignement majeur : la sécurité du 21^{ème} siècle ne peut plus être pensée comme la seule capacité de l'État à répondre aux crises lorsqu'elles surviennent. Elle repose désormais sur son aptitude à les anticiper, à en limiter les conséquences et à assurer la continuité des fonctions essentielles de la Nation.

Les travaux conduits montrent que les frontières entre sécurité intérieure, cybersécurité, protection des infrastructures critiques, prévention, renseignement, défense et souveraineté numérique deviennent de plus en plus perméables. Une attaque informatique peut aujourd'hui désorganiser un hôpital, interrompre un service public, fragiliser une entreprise ou compromettre le fonctionnement d'une collectivité territoriale avec des conséquences aussi importantes qu'une crise de sécurité classique. La protection des personnes ne peut donc plus être dissociée de celle des réseaux, des données et des organisations.

Cette évolution conduit également à dépasser une vision strictement régalienne de la sécurité. L'État demeure le garant de la protection des citoyens, mais il ne peut agir seul. Les collectivités territoriales, les entreprises, les opérateurs d'infrastructures critiques, les établissements d'enseignement, les associations et les citoyens participent désormais, chacun dans leur domaine, à la résilience du pays. La sécurité devient une responsabilité partagée.

La Commission en tire une conviction forte : la véritable puissance d'une Nation ne se mesure plus uniquement à ses effectifs, à ses équipements ou à ses capacités d'intervention. Elle se mesure également à sa capacité d'anticipation, à la qualité de sa coordination, au niveau de préparation de ses territoires, à la maîtrise de ses technologies critiques et aux compétences de celles et ceux qui les mettent en œuvre.

Ainsi comprise, la sécurité ne consiste plus seulement à protéger le territoire ; elle vise à garantir la continuité de la vie nationale dans un environnement marqué par l'incertitude, l'accélération technologique et la multiplication des crises. La résilience devient l'expression contemporaine de la souveraineté.

Cette évolution appelle naturellement une nouvelle étape. Après avoir établi ce diagnostic, la Commission formule dans la troisième partie de ce Cahier des recommandations destinées à renforcer durablement l'efficacité de notre politique de sécurité. Leur ambition est claire : permettre à la France de mieux protéger ses citoyens, de préserver ses libertés et de consolider sa souveraineté face aux défis du 21^{ème} siècle.

* * *

UNE AMBITION POUR 2030 - Construire une France plus sûre, plus résiliente et plus souveraine

À l'horizon 2030, la France devra être en mesure d'assurer à chacun de ses citoyens une sécurité qui ne se limite plus à la protection contre les menaces, mais qui garantisse également la continuité de la vie collective, la confiance dans les institutions et la capacité de la Nation à faire face aux crises.

Dans un monde marqué par les tensions géopolitiques, les attaques hybrides, les risques cyber, les catastrophes naturelles et les bouleversements technologiques, la sécurité ne pourra plus être pensée comme une politique sectorielle. Elle devra irriguer l'ensemble de l'action publique, depuis l'éducation et la prévention jusqu'à la justice, la cybersécurité, la protection civile, la souveraineté numérique et la résilience des territoires.

Cette ambition repose sur une conviction simple : une Nation est d'autant plus forte qu'elle est capable d'anticiper les crises, d'y résister et de retrouver rapidement son fonctionnement normal. La résilience devient ainsi un objectif stratégique au même titre que la sécurité ou la défense. Elle suppose des institutions efficaces, des infrastructures protégées, des services publics préparés, des entreprises mobilisées et des citoyens pleinement acteurs de leur propre sécurité.

Construire une France plus sûre, plus résiliente et plus souveraine suppose notamment de :

- Renforcer durablement les capacités des forces de sécurité intérieure et de la justice afin de garantir partout l'effectivité de l'État de droit ;
- Faire de la prévention une politique publique à part entière, en agissant en amont sur les facteurs de délinquance, de radicalisation et de vulnérabilité ;
- Protéger les infrastructures critiques, les données stratégiques et les services essentiels face aux menaces numériques et hybrides ;
- Développer une véritable culture nationale de la résilience, associant l'État, les collectivités territoriales, les entreprises, les associations et les citoyens ;
- Consolider la souveraineté technologique de la France et de l'Europe dans les domaines stratégiques, notamment le numérique, l'intelligence artificielle et la cybersécurité ;
- Renforcer la coopération européenne et internationale afin de répondre à des menaces qui ignorent désormais les frontières.

À l'horizon 2030, l'ambition n'est pas seulement de disposer de moyens supplémentaires. Elle est de bâtir une politique de sécurité plus cohérente, plus anticipatrice et plus résiliente, capable de protéger durablement les Français, de

préserver leurs libertés et de garantir la continuité de la Nation face aux défis du 21^{ème} siècle.

* * *

LES RECOMMANDATIONS DE LA COMMISSION

Cinq recommandations prioritaires

Au terme de ses travaux, la Commission considère que la France dispose de nombreux atouts pour assurer la sécurité de ses citoyens : des forces de sécurité reconnues, une justice indépendante, des services de renseignement performants, une expertise de haut niveau en matière de cybersécurité et un tissu industriel capable de soutenir l'innovation.

Pourtant, ces moyens ne produisent pas toujours les résultats attendus. Les difficultés observées tiennent moins à l'absence de dispositifs qu'à la complexité des organisations, au cloisonnement des acteurs, à l'insuffisante continuité de l'action publique et à la difficulté de transformer les ressources mobilisées en résultats visibles pour les citoyens.

La Commission estime dès lors que la priorité ne doit pas être de multiplier les structures ou les réformes ponctuelles, mais de rendre l'action publique plus simple, plus coordonnée, plus anticipatrice et plus efficace.

Les recommandations formulées dans ce Cahier répondent à cette exigence. Elles poursuivent une même ambition : mieux protéger les Français tout en garantissant les libertés publiques, l'autorité de l'État de droit et la souveraineté de la Nation.

Elles s'articulent autour de cinq priorités complémentaires :

1. Restaurer l'efficacité de la sécurité intérieure ;
2. Rendre la chaîne pénale plus rapide et plus lisible ;
3. Faire de la prévention un pilier de la politique de sécurité ;
4. Faire de la cybersécurité une politique de puissance ;
5. Renforcer la souveraineté française et européenne.

Ces cinq recommandations ne constituent pas des politiques indépendantes. Elles forment les composantes d'une même stratégie de sécurité globale. L'efficacité des forces de sécurité dépend de la crédibilité de la réponse judiciaire ; la prévention contribue à réduire durablement les violences et la récidive ; la cybersécurité protège la continuité des services essentiels ; la souveraineté technologique garantit à la France et à l'Europe leur liberté d'action.

La Commission appelle ainsi à inscrire ces orientations dans le temps long, à leur attribuer des responsabilités clairement identifiées et à évaluer régulièrement leurs effets concrets sur la sécurité des citoyens, la résilience des territoires et la confiance dans les institutions.

Les principales actions proposées

Afin de traduire ces orientations en résultats concrets, la Commission identifie plusieurs actions prioritaires susceptibles d'être engagées à court et moyen terme. Elles ne constituent pas un programme exhaustif, mais un socle d'actions cohérent permettant d'améliorer durablement l'efficacité de la politique de sécurité.

1. Simplifier l'action des forces de sécurité

- Recentrer policiers et gendarmes sur leurs missions opérationnelles.
- Alléger les tâches administratives grâce à la simplification des procédures et au développement des outils numériques.
- Renforcer la présence visible des forces de sécurité sur le terrain.
- Développer les formations communes entre forces de sécurité, magistrats et spécialistes du numérique.

2. Accélérer le fonctionnement de la chaîne pénale

- Simplifier certaines procédures judiciaires.
- Réduire les délais de traitement des affaires.
- Améliorer le suivi et l'exécution effective des décisions de justice.
- Renforcer la coordination entre police, gendarmerie, justice et administration pénitentiaire.
- Poursuivre la modernisation de la politique pénitentiaire afin de mieux prévenir la récidive.

3. Développer une véritable politique de prévention

- Renforcer les actions éducatives et le soutien à la parentalité.
- Développer les dispositifs de médiation et de prévention de proximité.
- Mieux coordonner les acteurs éducatifs, sociaux, sanitaires et judiciaires.
- Renforcer les actions de prévention des addictions, des ruptures sociales et de la récidive.
- Encourager les dispositifs favorisant la réinsertion et, lorsque les situations s'y prêtent, les démarches de justice restaurative.

4. Renforcer la résilience numérique de la Nation

- Généraliser la sensibilisation à la cybersécurité dans les administrations.
- Développer des parcours de formation adaptés aux différents niveaux de responsabilité.
- Consolider les capacités nationales de prévention, de détection et de réponse aux incidents.
- Accompagner les collectivités territoriales et les opérateurs essentiels dans le renforcement de leur sécurité numérique.
- Organiser régulièrement des exercices de gestion de crise cyber.

5. Consolider la souveraineté technologique

- Soutenir une filière française et européenne de cybersécurité.
- Encourager le recours aux technologies de confiance dans les politiques publiques.
- Réduire les dépendances technologiques critiques.
- Renforcer les coopérations européennes en matière de cybersécurité, de partage d'information et de gestion des crises.
- Développer une culture de l'évaluation afin de mesurer régulièrement l'efficacité des politiques de sécurité.

Ces actions traduisent une même ambition : faire évoluer la politique de sécurité vers un modèle plus simple, plus coordonné, plus anticipateur et davantage orienté vers les résultats. Leur réussite repose moins sur la création de nouveaux dispositifs que sur une meilleure mobilisation des moyens existants, une coopération renforcée entre les acteurs et une évaluation régulière des politiques publiques.

* * *

CONCLUSION

Protéger aujourd'hui, préparer demain

Au terme de ses travaux, la Commission est parvenue à une conviction essentielle : la sécurité est l'une des conditions de la confiance démocratique. Elle garantit l'exercice des libertés, assure l'effectivité de l'État de droit et permet à la Nation de se projeter avec confiance dans l'avenir.

Or cette mission ne peut plus être pensée selon les catégories du passé. Les menaces contemporaines ignorent les frontières administratives, territoriales ou technologiques. Elles appellent une réponse globale, associant sécurité intérieure, justice, prévention, cybersécurité, protection des infrastructures critiques, souveraineté numérique et résilience nationale.

La France dispose pour relever ce défi d'atouts considérables : des institutions solides, des forces de sécurité et des magistrats reconnus, des services de renseignement performants, une expertise de haut niveau en matière de cybersécurité ainsi qu'une tradition républicaine fondée sur la primauté du droit. L'enjeu n'est donc pas de reconstruire un modèle, mais de le rendre plus cohérent, plus lisible et plus efficace.

Les travaux de la Commission conduisent à privilégier une approche fondée sur quatre exigences complémentaires : renforcer l'autorité de l'État de droit, mieux coordonner l'action publique, développer une véritable culture de la prévention et inscrire la résilience au cœur de notre stratégie nationale. La sécurité de demain se gagnera moins par l'accumulation de dispositifs que par la capacité de l'ensemble des acteurs à agir de manière coordonnée, anticipatrice et durable.

Cette ambition dépasse la seule responsabilité des forces de sécurité. Elle engage l'État, les collectivités territoriales, les entreprises, les établissements d'enseignement, les associations et les citoyens eux-mêmes. Dans une société plus exposée aux crises, la sécurité devient un bien commun dont chacun est à la fois bénéficiaire et acteur.

Protéger les Français, préserver leurs libertés et garantir la continuité de la Nation constituent aujourd'hui une même exigence. C'est à cette condition que la France pourra affronter les défis du 21^{ème} siècle avec confiance, renforcer sa souveraineté et transmettre aux générations futures une République plus sûre, plus résiliente et plus forte.

* * *

ANNEXES

Annexe 1 — La Commission : méthode de travail et composition

Les travaux de la Commission « Sécurité » ont été conduits entre septembre 2025 et juin 2026 sous l'égide du Cercle Avenir & Progrès. Ils se sont appuyés sur une méthode associant réflexion collective, analyses documentaires, auditions d'experts et échanges avec des praticiens issus des principaux domaines concernés par les politiques de sécurité.

La Commission a notamment mobilisé :

- Les contributions de ses membres ;
- Plusieurs réunions de travail consacrées aux différentes dimensions de la sécurité intérieure et de la protection des citoyens ;
- Des auditions de responsables publics, de praticiens et d'experts ;
- Les notes de travail et documents de synthèse élaborés par le groupe de travail ;
- Une revue de littérature française, européenne et internationale portant sur les politiques de sécurité, de justice, de prévention, de cybersécurité et de résilience.

Les travaux ont été conduits selon quatre principes :

- Partir des réalités observées et des données disponibles ;
- Croiser les approches institutionnelles, opérationnelles et académiques ;
- Inscrire la réflexion dans une perspective républicaine et européenne ;
- Formuler des propositions concrètes, opérationnelles et soutenables.

Composition de la Commission

La Commission « Sécurité » rassemble des membres du Cercle Avenir & Progrès aux parcours complémentaires. Cette diversité constitue l'une des richesses de ses travaux et permet de croiser les regards.

Elle a été présidée par **Gilbert Metoudi et Michel Ruimy**

Le Cercle Avenir & Progrès remercie l'ensemble des membres de la Commission ainsi que les nombreuses personnalités qui ont accepté de contribuer à ses travaux par leurs analyses, leurs retours d'expérience et leurs propositions. Ces échanges ont permis d'enrichir la réflexion collective et de nourrir les recommandations présentées dans ce Cahier.

Annexe 2 — Les auditions et contributions ayant nourri les travaux de la Commission

Un temps fort de la réflexion du Cercle Avenir & Progrès

Les travaux de la Commission « Sécurité » se sont appuyés sur les contributions de ses membres, sur l'analyse de nombreux rapports publics ainsi que sur les échanges conduits avec des praticiens, des responsables publics et des experts des questions de sécurité.

Cette méthode de travail avait un double objectif : confronter les analyses théoriques aux réalités du terrain et faire émerger des propositions opérationnelles répondant aux défis contemporains de la sécurité.

Les échanges ont porté notamment sur :

- L'évolution de la délinquance et du sentiment d'insécurité ;
- Les transformations de la menace terroriste et du narcotrafic ;
- Les relations entre sécurité, justice et prévention ;
- La cybersécurité et les nouvelles formes de criminalité ;
- Les enjeux de souveraineté numérique et de protection des infrastructures critiques ;
- Les comparaisons européennes en matière de politiques de sécurité.

Les principaux enseignements

- **Une sécurité devenue globale.** Les risques contemporains dépassent largement les seules questions d'ordre public et concernent également le cyberspace, les infrastructures critiques, les crises sanitaires, les risques informationnels et les atteintes à la cohésion nationale.
- **Une exigence d'efficacité de l'action publique.** Les citoyens attendent une réponse rapide, lisible et cohérente des pouvoirs publics, fondée sur une meilleure coordination entre les différents acteurs de la sécurité.
- **La prévention comme complément indispensable de la répression.** Les politiques de sécurité ne peuvent produire des résultats durables sans agir simultanément sur les causes de la délinquance, l'éducation, la prévention de la récidive et la protection des publics les plus vulnérables.
- **Une approche européenne indispensable.** Face à des menaces largement transnationales, la coopération européenne constitue un levier essentiel pour renforcer l'efficacité des politiques de sécurité, qu'il s'agisse de lutte contre le terrorisme, de criminalité organisée, de cybersécurité ou de contrôle des frontières.

Les auditions, contributions et échanges conduits tout au long des travaux ont constitué un apport déterminant à la réflexion de la Commission et ont directement nourri les analyses ainsi que les recommandations présentées dans ce Cahier.

Annexe 3 — Les principaux textes juridiques de référence

Les travaux de la Commission « Sécurité » s'inscrivent dans le cadre des principaux textes qui organisent la sécurité intérieure, garantissent les libertés publiques, définissent les règles de la procédure pénale et encadrent la prévention des nouvelles menaces, notamment terroristes, numériques et cybercriminelles.

Droit français

- Constitution du 4 octobre 1958, notamment ses dispositions relatives à la protection des libertés, à l'autorité judiciaire et aux pouvoirs publics en période de crise ;
- Déclaration des droits de l'homme et du citoyen du 26 août 1789, notamment :
- Article 2, qui reconnaît la sûreté parmi les droits naturels et imprescriptibles de l'homme ;
- Article 12, relatif à la nécessité d'une force publique instituée pour l'avantage de tous ;
- Articles 7 à 9, relatifs à la légalité des poursuites, à la présomption d'innocence et à la nécessité des peines ;
- Code de la sécurité intérieure, qui définit les principes généraux et l'organisation de la sécurité intérieure, les missions des forces de sécurité, la sécurité civile, le renseignement, la prévention du terrorisme ainsi que les pouvoirs de police administrative ;
- Code pénal, notamment les dispositions relatives :
 - Aux atteintes aux personnes et aux biens ;
 - Au terrorisme et à la criminalité organisée ;
 - Aux atteintes aux intérêts fondamentaux de la Nation ;
 - Aux atteintes aux systèmes de traitement automatisé de données ;
- Code de procédure pénale, qui encadre les enquêtes, les poursuites, le jugement des infractions, les droits des victimes et des personnes mises en cause ainsi que l'exécution des peines ;
- Code de la justice pénale des mineurs, relatif à la responsabilité pénale des mineurs, à leur prise en charge éducative et aux réponses judiciaires applicables ;
- Code de la défense, notamment ses dispositions relatives à la sécurité nationale, à la protection des activités d'importance vitale, à la cyberdéfense et à la continuité des fonctions essentielles de la Nation ;

- Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, qui définit le cadre juridique des techniques de renseignement et leur contrôle ;
- Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, dite loi SILT ;
- Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025, notamment ses dispositions ayant renforcé la protection des systèmes d'information et des opérateurs essentiels ;
- Loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'Intérieur, qui programme l'évolution des moyens, de l'organisation et de la transformation numérique du ministère de l'Intérieur
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, qui encadre le traitement des données personnelles, notamment dans le domaine de la sécurité et de la justice.

Droit européen

- Traité sur l'Union européenne, notamment son article 4, paragraphe 2, qui rappelle que la sécurité nationale demeure de la responsabilité de chaque État membre ;
- Traité sur le fonctionnement de l'Union européenne, notamment son titre V consacré à l'espace de liberté, de sécurité et de justice et à la coopération policière et judiciaire en matière pénale ;
- Charte des droits fondamentaux de l'Union européenne, notamment les dispositions relatives :
 - Au droit à la liberté et à la sûreté ;
 - Au respect de la vie privée ;
 - À la protection des données personnelles ;
 - Au droit à un recours effectif et à un procès équitable ;
 - À la présomption d'innocence et aux principes de légalité et de proportionnalité des délits et des peines ;
- Règlement (UE) 2016/794 relatif à Europol, qui organise la coopération de l'Agence de l'Union européenne pour la coopération des services répressifs ;
- Directive (UE) 2016/680, relative à la protection des données personnelles traitées par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquête et de poursuites ;
- Directive (UE) 2017/541 relative à la lutte contre le terrorisme ;
- Règlement (UE) 2019/881, dit Cybersecurity Act, relatif à l'Agence de l'Union européenne pour la cybersécurité — ENISA — et à la certification européenne de cybersécurité ;

- Directive (UE) 2022/2555, dite directive NIS 2, concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union ;
- Directive (UE) 2022/2557 relative à la résilience des entités critiques, qui renforce la protection et la continuité des services essentiels ;
- Décision-cadre 2002/584/JAI relative au mandat d'arrêt européen, qui facilite la remise des personnes recherchées entre les autorités judiciaires des États membres.

Références internationales

- **Déclaration universelle des droits de l'homme du 10 décembre 1948**, notamment ses dispositions relatives à la sûreté, à la protection contre les arrestations arbitraires, à la présomption d'innocence et au droit à un procès équitable ;
- **Pacte international relatif aux droits civils et politiques du 16 décembre 1966**, relatif notamment au droit à la sécurité, aux garanties judiciaires et à la protection des libertés fondamentales ;
- **Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950**, notamment ses articles 5, 6, 7 et 8 relatifs à la liberté et à la sûreté, au procès équitable, à la légalité des peines et au respect de la vie privée ;
- **Convention des Nations unies contre la criminalité transnationale organisée du 15 novembre 2000, dite Convention de Palerme**, ainsi que ses protocoles additionnels relatifs à la traite des personnes, au trafic illicite de migrants et au trafic d'armes à feu ;
- **Convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001, dite Convention de Budapest**, et ses protocoles additionnels relatifs aux actes racistes et xénophobes commis par l'intermédiaire de systèmes informatiques ainsi qu'à la coopération et à l'accès aux preuves électroniques ;
- **Convention des Nations unies contre la corruption du 31 octobre 2003, dite Convention de Mérida** ;
- **Résolutions du Conseil de sécurité des Nations unies relatives à la lutte contre le terrorisme**, à son financement et à la coopération internationale en matière de sécurité ;
- **Convention des Nations unies contre la cybercriminalité du 24 décembre 2024**, consacrée à la coopération internationale contre les infractions commises au moyen des technologies de l'information et au partage des preuves électroniques. À la date de juillet 2026, cette **convention est signée mais n'est pas encore entrée en vigueur**.

Annexe 4 — Bibliographie sélective

Les travaux de la Commission « Sécurité » se sont appuyés sur des ouvrages, études et rapports consacrés à la sécurité intérieure, à l'organisation des forces de sécurité, à la chaîne pénale, à la prévention, à la cybercriminalité et à la résilience nationale.

Sécurité intérieure, police et société

- **LAUZE Frédéric et PLOQUIN Frédéric**, *Insécurité. Stop à la descente aux enfers*, Fayard, 2025.
- **DE MAILLARD Jacques et SKOGAN Wesley**, *Police et société en France*, Presses de Sciences Po, 2023.
- **OCQUETEAU Frédéric**, *Mais qui donc dirige la police ? Sociologie des commissaires*, Armand Colin, 2006.
- **VALLAR Christian et VENTRE André-Michel**, *Le Commissaire de police*, L'Harmattan, collection « Sécurité et société », 2021.
- **FILLIEULE Olivier et JOBARD Fabien**, *Politiques du désordre. La police des manifestations en France*, Seuil, 2020.

Politiques publiques et organisation de la sécurité

- Ministère de l'Intérieur, *Livre blanc de la sécurité intérieure*, 2020.
- Cour des comptes, **rapports consacrés aux forces de sécurité intérieure, à la Police nationale, à la Gendarmerie nationale et à l'organisation territoriale de la sécurité.**
- Service statistique ministériel de la sécurité intérieure — SSMSI, **rapports annuels *Insécurité et délinquance*, ministère de l'Intérieur.**
- Institut des hautes études du ministère de l'Intérieur — IHEMI, **études et travaux consacrés à la sécurité intérieure, à la gestion des crises, à la résilience et aux nouvelles menaces.**

Justice, criminalité et prévention

- Ministère de la Justice, **rapports annuels et statistiques consacrés à l'activité des juridictions, à l'exécution des peines, à l'administration pénitentiaire et à la récidive.**
- Observatoire national de la délinquance et des réponses pénales, ***La Criminalité en France*, rapports annuels, CNRS Éditions. Ces travaux rappellent notamment la nécessité de distinguer les faits enregistrés par les services de sécurité de l'ensemble des faits réellement subis par la population.**

- Observatoire français des drogues et des tendances addictives — OFDT, **rapports consacrés aux marchés des drogues, aux trafics et aux politiques de prévention.**

Cybersécurité et nouvelles menaces

- Agence nationale de la sécurité des systèmes d'information — ANSSI, *Panorama de la cybermenace*, publication annuelle.
- ANSSI, stratégies nationales et guides relatifs à la cybersécurité, à la protection des systèmes d'information et à la gestion des crises numériques.
- Europol, *European Union Serious and Organised Crime Threat Assessment — EU-SOCTA*, rapports consacrés à la criminalité organisée et aux menaces transnationales.
- Agence de l'Union européenne pour la cybersécurité — ENISA, rapports sur l'état de la menace cyber, la résilience des infrastructures critiques et la mise en œuvre du cadre européen de cybersécurité.
- BERTHET Vincent et AMSELLEM Léo, *Les Nouveaux Oracles. Comment les algorithmes prédisent le crime*, CNRS Éditions, 2021.

*** **

Penser. Débattre. Agir pour faire société.

Le Cercle Avenir & Progrès

Première édition des Cahiers 2026