RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

STRATÉGIE GIP ACYMA 2025-2030

www.cybermalveillance.gouv.fr

AVANT-PROPOS

Depuis 2017, le dispositif Cybermalveillance.gouv.fr a largement démontré sa capacité à répondre au besoin d'assistance, de sensibilisation et d'observation de la menace avec notamment plus d'1 million de victimes assistées, 500 contenus produits (campagnes vidéo, guides, fiches pratiques, fiches réflexe, alertes, etc.) et 15 millions de visiteurs sur la plateforme depuis l'origine. Pourtant, si notre démarche a fait ses preuves et s'ancre peu à peu dans l'esprit des Français, il reste encore beaucoup à accomplir pour répondre aux enjeux de demain, à l'évolution des cybermenaces et au passage au tout numérique de la société.

Fort de sa position centrale acquise au sein de l'écosystème cyber et de sa légitimité auprès des autorités gouvernementales et de ses publics, Cybermalveillance.gouv.fr s'est vu confier un rôle déterminant dans la conduite de projets nationaux ambitieux, tel que l'équivalent numérique du 17, le 17Cyber, qui permettra de mieux assister les victimes de cybermalveillance.

La stratégie à 5 ans du groupement d'intérêt public (GIP) ACYMA se veut donc ambitieuse. Le GIP s'efforce d'y apporter la valeur ajoutée maximale à ses principales parties prenantes : les victimes (particuliers, entreprises/ associations et les collectivités), ses membres, ses prestataires référencés et labellisés et l'ensemble de l'écosystème pour les années à venir.
C'est dans cet élan, et afin d'être en capacité de relever les défis à venir, que le GIP ACYMA a défini sa première stratégie à 5 ans. Certaines contraintes et incertitudes auront bien sûr un impact sur la mise en place et le déroulement des éléments de la stratégie. Ainsi, l'évolution très rapide de la menace cyber et la réponse collective qui y est apportée ainsi que les évolutions réglementaires et de l'écosystème et les différentes politiques publiques cyber mises en œuvre par l'État devront être anticipées et prises en compte. La stratégie du GIP doit donc, comme depuis sa création, être considérée comme un document évolutif, mis à jour annuellement et décliné en programmes d'activités du GIP en fonction des moyens qui lui seront alloués.

Ce document présente le contexte, la méthodologie retenue, le bilan, un projet phare du GIP puis les objectifs stratégiques retenus.

CONTEXTE

Pour rappel, les missions actuelles du GIP sont définies dans sa convention. Le Groupement a pour objet d'assurer une mission d'intérêt général de lutte contre les cybermenaces, portant en particulier sur la prévention, l'accompagnement et l'assistance aux particuliers, aux entreprises, aux associations et aux administrations victimes d'actes de cybermalveillance par la mise en place d'un « guichet unique ». Plus particulièrement, le groupement s'attachera d'une part, à permettre la mise en relation avec des acteurs de proximité capables de procéder à la sécurisation et à la reprise d'activité des victimes et d'autre part, à fournir l'aide aux démarches administratives requises pour le dépôt de plainte ; la sensibilisation du public sur les enjeux de la sécurité et de la protection de la vie privée numérique en lien avec les autorités compétentes et le développement de campagnes de prévention en la matière ; la fourniture d'éléments statistiques offrant une vue réelle et consolidée de la menace cyber afin de mieux l'anticiper à travers la création d'un observatoire dédié.

La Cour des Comptes a procédé à un contrôle des comptes et de la gestion du GIP sur les exercices 2017 à 2020 et a rendu publiques ses conclusions qui avaient conduit à différents constats et recommandations :

Constats :

- « *Les ressources humaines et financières actuelles du groupement paraissent insuffisantes pour répondre aux missions et atteindre les objectifs qui lui ont été confiés par ses membres et par ses tutelles. Elles doivent pouvoir être stabilisées et devenir pérennes.* »
- « *Faute de moyens supplémentaires, les ambitions du GIP ne pourront qu'être revues à la baisse ce qui paraîtrait paradoxal dans un contexte de croissance soutenue des cybermenaces, sauf à envisager d'autres solutions pour couvrir un besoin bien réel et porteur d'enjeux stratégiques pour la France.* »
- « *Le GIP complète donc l'offre de l'État en fournissant une réponse technique et pratique à un public hors OIV/OSE au niveau local qui se trouve démuni devant une agression cyber. La force du GIP réside dans sa capacité à faire le lien, via son réseau de partenaires et de prestataires, entre la victime potentielle, les services des ministères de l'intérieur et de la justice, et les sociétés capables d'apporter rapidement une solution au problème rencontré.* »

Recommandations :

- Recommandation n° 5 (SGG, SGDSN, ANSSI, GIP). Mettre en place des ressources financières pérennes pour assurer les missions du GIP ACYMA, en étudiant toutes les solutions publiques et privées.
- Recommandation n° 6 (SGG, SGDSN, ANSSI, GIP). Élaborer un plan stratégique à cinq ans pour l'évolution du GIP ACYMA après 2022, en cohérence avec la stratégie nationale de cybersécurité.

MÉTHODOLOGIE DE L'ÉLABORATION DE
LA STRATÉGIE À 5 ANS

Le GIP a réuni ses membres en groupe de travail entre mi-2023 et début 2024 afin qu'ils puissent établir cette stratégie à 5 ans.

Le groupe de travail était composé des administrateurs du GIP, des représentants des collèges en Assemblée générale et des représentants des membres étatiques.

Des personnalités qualifiées ont été consultées (délégation à la sécurité routière et service d'information du Gouvernement) lors des échanges sur la notoriété du GIP.

Le GIP, avec le soutien de l'ANSSI, a organisé les réunions en présentiel ainsi que le programme de travail préparatoire.

Après l'établissement d'un bilan, les membres ont été invités à travailler sur 3 axes :

Axe de travail n° 1
Notoriété du GIP ACYMA - élever le GIP ACYMA au rang de référence de l'assistance aux victimes de cybermalveillance.

Axe de travail n° 2
Mobilisation des services de l'État et de l'écosystème autour du GIP ACYMA.

Axe de travail n° 3
Gouvernance du GIP.

De premiers objectifs stratégiques ont été soumis lors d'une réunion avec les membres des cabinets ministériels en septembre 2023, qui a permis de valider ces premières orientations.

BILAN DES ACTIVITÉS DU GIP **DEPUIS 2017**

Constats majeurs
Les travaux ont permis d'identifier plusieurs constats majeurs :

- le GIP a démontré son efficacité depuis sa création. Il s'inscrit pleinement dans l'écosystème public et privé de lutte contre la cybermalveillance. Il parvient à toucher des populations au-delà de l'écosystème cyber traditionnel. Il a démontré son expertise dans la mise en relation entre les victimes et les prestataires ;

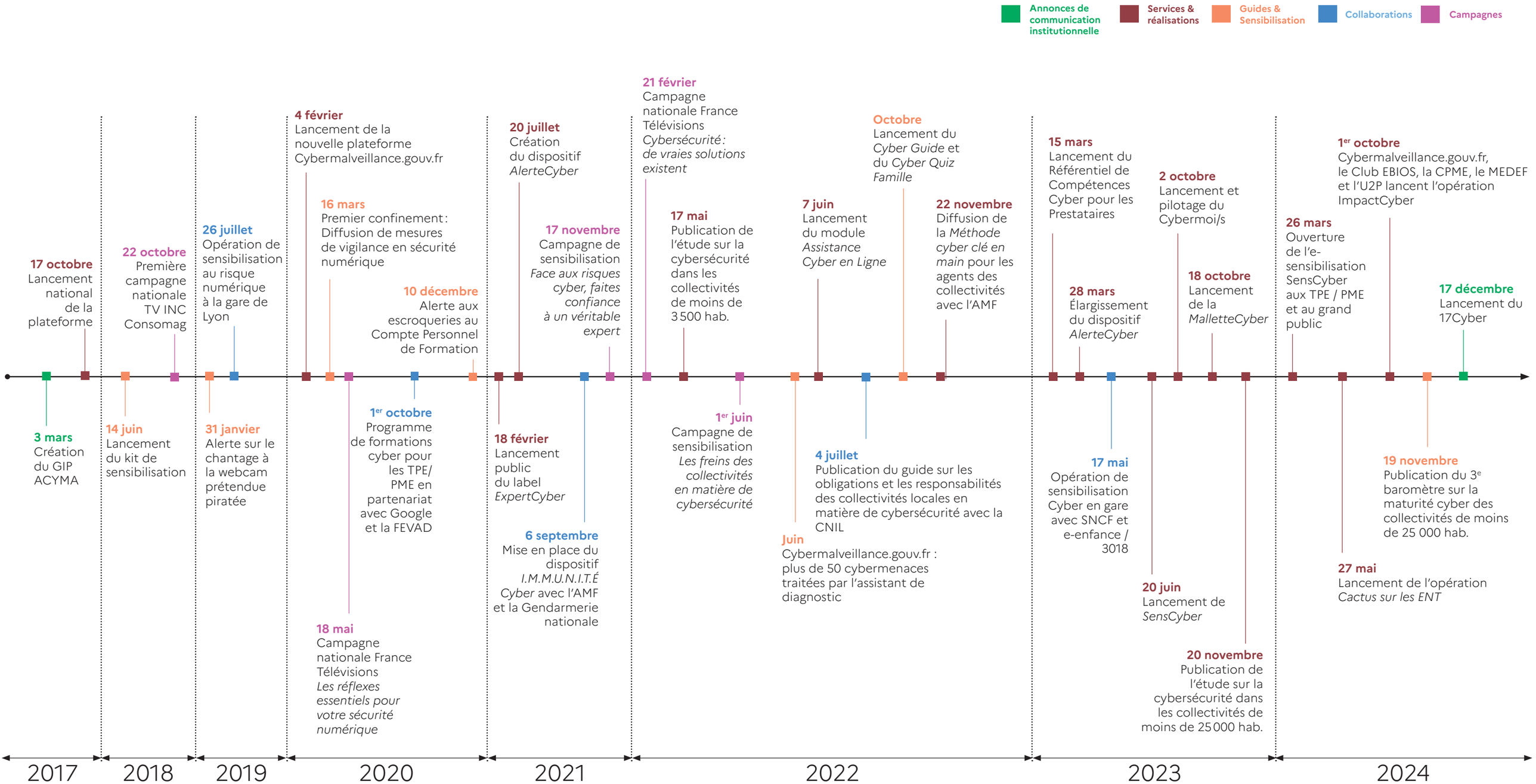
- sa forme juridique de Groupement d'Intérêt Public est très adaptée aux missions confiées, même si elle impose quelques contraintes qui sont surmontées ;

- sa notoriété n'est pas encore suffisante, du fait du manque de moyens humains et financiers, par rapport aux enjeux de lutte contre la cybermalveillance pour les différents publics. De même, l'ensemble des services proposés par le GIP n'est pas suffisamment connu par ses bénéficiaires directs, ni visible du reste de l'écosystème cyber ;

- ses moyens doivent être renforcés pour lui permettre de réaliser les missions qui lui ont été confiées – par exemple la réalisation de campagnes de prévention.

RÉALISATIONS MAJEURES DU GIP

DEPUIS 2017



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

ORIENTATIONS STRATÉGIQUES

La raison d'être du GIP ACYMA est sa capacité à guider les citoyens et organisations vers des acteurs compétents pour les accompagner dans leurs démarches face à la cybermalveillance.

Pour poursuivre et prolonger cette mission, le GIP ACYMA doit désormais devenir une porte d'entrée connue du plus grand nombre.

Pour cela, une logique de marque doit accompagner le développement et la promotion de ses activités. Le GIP doit également développer des interfaces de mise en relation avec les acteurs compétents en s'appuyant sur une logique de marques sur chacun de ses champs d'action :

- l'assistance aux victimes ;
- la prévention cyber ;
- le signalement.

Pour remplir ces objectifs stratégiques, comme indiqué en avant-propos, le GIP proposera chaque année un programme d'activités. Des indicateurs seront définis dans le programme d'activités et suivis annuellement. Ils permettront d'évaluer la mise en œuvre des objectifs stratégiques et d'ajuster au besoin les axes de travail du GIP.

OBJECTIF STRATÉGIQUE 1

Faire du 17Cyber la marque du GIP ACYMA

pour l'assistance aux victimes de cybermalveillances

Il s'agit d'affirmer le positionnement du GIP dans l'assistance aux victimes de cybermalveillance en faisant connaître la marque et les services du 17Cyber à l'ensemble des publics du GIP et en articulant l'action du GIP avec celle des acteurs (sectoriels et territoriaux) de l'assistance aux victimes.

Le projet 17Cyber est porté par le ministère de l'Intérieur et des Outre-mer. Le GIP a été sollicité pour porter l'optimisation de la plateforme déjà mise en place (Cybermalveillance.gouv.fr), permettant l'accompagnement et la réorientation des victimes d'une part, vers des acteurs en capacité d'offrir une réponse technique adaptée aux fins notamment de remédiation ou de collecte de données d'incidentologie, et, d'autre part, vers les services de la police ou de la gendarmerie nationale ou des services du procureur de la République compétent aux fins de signalement ou de dépôt de plainte. Le 17Cyber sera une porte d'entrée pour toutes les victimes de cybermalveillance : particuliers, entreprises, associations et collectivités.

La promotion de ces services doit s'accompagner de campagnes de communication massives et efficaces autour du « 17Cyber » incluant toutes les parties prenantes de l'assistance aux victimes.

OBJECTIF STRATÉGIQUE 2

Développer une marque dont l'identité reste à définir

pour les actions de prévention cyber afin de devenir un levier efficace des actions de communication gouvernementales sur le sujet

Il s'agit de positionner le GIP à l'intersection des communications liées à la prévention des risques cyber pour l'ensemble des publics.
Même si la marque Cybermalveillance.gouv.fr a démontré à plusieurs reprises sa capacité à réaliser des campagnes de prévention[1], un passage à l'échelle s'avère nécessaire compte tenu de l'ampleur que prennent les enjeux liés à la prévention des risques cyber. Garantir ce positionnement renforcé du GIP passera par une stratégie de marque qui pourrait s'appuyer sur deux leviers :

- la poursuite de la création de contenus de sensibilisation :
  - adaptés aux publics cibles ;
  - en veillant à réduire la fracture numérique territoriale ou générationnelle ;
  - en utilisant les supports de communication en adéquation avec les publics cibles (notamment réseaux sociaux ou professionnels) ;
  - en ayant une attention particulière pour les publics de décideurs (publics ou privés) qui sont moins familiers des enjeux de sécurité du numérique.
- le développement d'une marque reconnue et lisible qui pourrait être :
  - la marque historique « Cybermalveillance » ;
  - la marque de l'assistance aux victimes, le « 17Cyber » ;
  - ou une nouvelle marque à définir.

1 Consomag chaque année depuis sa création, campagne nationale *Les réflexes essentiels pour votre sécurité numérique* pendant le premier confinement, campagne *Face aux risques cyber, faites confiance à un véritable expert* pour la promotion du label ExpertCyber ou encore campagne *Les freins des collectivités en matière de cybersécurité* et *Les risques numériques à destination des élus*.

OBJECTIF STRATÉGIQUE 3

Explorer le développement d'un parcours de signalement

permettant de faciliter l'utilisation des dispositifs étatiques existants

Aujourd'hui les citoyens, entreprises, associations et collectivités territoriales ne savent pas vers quel dispositif se rapprocher lorsqu'ils souhaitent signaler un site malveillant, un SMS d'hameçonnage, une fraude ou bien déposer plainte en ligne ou directement auprès des services judiciaires compétents. En ce sens, plusieurs rapports parlementaires ou encore celui de la Cour des Comptes mentionnent : « *Au plan national, le foisonnement de services d'enquête en charge de la lutte contre la cybercriminalité et de plateformes de signalement apparaît difficilement lisible pour le citoyen et nécessite une coordination coûteuse en énergie et en temps* ».

Au même titre qu'être une porte d'entrée vers des services d'assistance, le GIP souhaite adresser le besoin de disposer d'une porte d'entrée pour effectuer des signalements pour une entité ou un individu afin d'informer les autorités étatiques compétentes, en tant que victime ou témoin, de toute action de cybermalveillance présumée ou avérée.

Sur la base de son parcours de diagnostic en ligne, le GIP pourrait ainsi orienter les victimes vers les plateformes de signalement ou de dépôt de plainte adéquates et préparer leurs déclarations afin de rendre ce parcours utilisateur aussi simple que possible. L'existence de ce service permettrait à la fois d'améliorer l'utilisation des dispositifs de signalement par les citoyens, mais aussi une meilleure collecte et centralisation des informations.

ZOOM SUR LE **17CYBER**

Le projet est porté par le ministère de l'Intérieur et des Outre-mer avec une implication forte de la direction générale de la police nationale et la direction générale de la gendarmerie, qui ont confié au GIP sa mise en œuvre technique.

Objectifs :

- un service d'assistance et d'orientation des victimes d'actes de cybermalveillance ;
- une solution utilisant les outils et services existants et immédiatement opérationnels pour optimiser le coût ;
- une meilleure observation de la menace grâce à la quantité et la qualité des données recueillies ;
- une livraison rapide d'une version fonctionnelle ;
- un service simple et accessible qui permette notamment un accompagnement vers la judiciarisation.

Le GIP ACYMA a été mobilisé dans le cadre d'une convention de cadrage afin de lui confier l'optimisation de la plateforme déjà mise en place (Cybermalveillance.gouv.fr), permettant l'accompagnement et la réorientation des victimes vers des services ou des acteurs en capacité de leur offrir une réponse adaptée.