Cour des comptes

QUATRIÈME CHAMBRE

S2022-0820

DEUXIÈME SECTION

OBSERVATIONS DÉFINITIVES

(Article R. 143-11 du code des juridictions financières)

GROUPEMENT D'INTÉRÊT PUBLIC D'ASSISTANCE AUX VICTIMES D'ACTES DE CYBERMALVEILLANCE (ACYMA)

Exercices 2017-2020

Le présent document, qui a fait l'objet d'une contradiction avec les destinataires concernés, a été délibéré par la Cour des comptes, le 16 mars 2022.

En application de l'article L. 143-1 du code des juridictions financières, la communication de ces observations est une prérogative de la Cour des comptes, qui a seule compétence pour arrêter la liste des destinataires.

TABLE DES MATIÈRES

SYNTHÈSE

Devant l'ampleur des cybermenaces et la recrudescence de la cybercriminalité, notamment depuis 2019 et pendant l'épidémie de COVID-19, la cybersécurité est devenue un enjeu stratégique pour la France et bénéficie, à ce titre, d'un effort significatif de la part du plan France Relance lancé en 2020.

Développé sur l'initiative et au sein de l'agence nationale de la sécurité des systèmes d'information (ANSSI) en 2016, le dispositif d'« assistance aux victimes d'actes de cybermalveillance (ACYMA) » est né du besoin de sensibiliser un plus large public, de nature très diverse, que les opérateurs d'intérêts vitaux (OIV) ou de services essentiels (OSE) déjà couverts par l'ANSSI. Il s'est traduit par la création en 2017 d'un groupement d'intérêt public (GIP), sous la tutelle du Premier ministre, du ministre de l'intérieur, du ministre de la justice, du ministre chargé de l'économie et des finances et du secrétaire d'État en charge du numérique. Le GIP ACYMA associe également des personnes morales de droit privé, membres fondateurs ou l'ayant rejoint par la suite. Au 31 décembre 2021, il compte 53 membres, emploie quatorze personnes à plein temps et dispose d'un réseau de 1 235 prestataires référencés sur le territoire national.

Cybermalveillance.gouv.fr : une réponse pertinente pour un besoin en croissance

Le GIP ACYMA a pour objectif de compléter la stratégie de cybersécurité française en s'adressant à des populations à la fois nombreuses, diffuses et vulnérables, pour lesquelles l'ANSSI n'apportait pas, en 2015, de réponse adaptée. Associant puissance publique, organismes publics, collectivités et acteurs privés, le GIP ne connaît pas d'équivalent au plan européen voire international.

Durant sa phase de montée en puissance, l'activité du GIP s'est prioritairement portée sur les volets « prévention » et « assistance » de sa mission, se limitant, dans le volet « anticipation et observation », à fournir aux services concernés du ministère de l'intérieur et du ministère de la justice des éléments statistiques issus de l'exploitation de sa plateforme *cybermalveillance.gouv.fr*. En dépit d'une activité en forte croissance ces deux dernières années, la notoriété du GIP et de sa plateforme d'accès à l'information reste limitée et l'observatoire de la menace reste à construire.

La coopération internationale, indispensable compte tenu du caractère transnational de cette menace, a été efficace notamment pour élaborer des instruments juridiques adaptés. 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. De même, la modestie des moyens que la justice consacre à cette menace contraste avec sa croissance. Le continuum du traitement judiciaire des actes de cybermalveillance, entre les forces de sécurité et le ministère de la justice, mériterait d'être consolidé, avec notamment le déploiement, attendu depuis le printemps 2020, de la possibilité d'effectuer des plaintes en ligne.

Des ressources à renforcer et à pérenniser pour atteindre les objectifs initiaux

Le GIP a réussi à respecter l'obligation statutaire de maintien à l'équilibre de ses comptes y compris durant l'épidémie de Covid-19 mais au détriment du budget consacré à la communication, pourtant cruciale pour asseoir et accroître sa notoriété. Les investissements

effectués par le GIP, notamment au profit de sa plateforme d'assistance, lui ont permis d'atteindre un premier palier opérationnel en 2020 au regard des ambitions visées, avec le développement de campagnes de sensibilisation sur le danger cyber et de produits d'information, conjugué au renforcement de l'offre de services et d'accompagnement des victimes.

Le groupement reste largement dépendant de la puissance publique, dans sa gouvernance comme dans son financement, alors que l'objectif principal d'un GIP est d'obtenir des partenaires privés des ressources financières significatives permettant de financer la mission d'intérêt général dans un contexte budgétaire contraint. La participation publique dans le GIP reste donc essentielle pour assurer la place accordée dans tous les documents stratégiques au concept *Cybermalveillance.gouv.fr* dans la perspective d'une complémentarité avec les missions dévolues à l'ANSSI.

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. Aucune piste ne doit être écartée *a priori*, au-delà des dons et des leviers plus classiques constitués par les subventions publiques et l'accroissement en nombre, en qualité et en montant unitaire des contributions des membres.

Un positionnement à préciser et une stratégie à élaborer au-delà de 2022

La stratégie nationale de cybersécurité de 2015 et les objectifs annoncés en février 2021 par le gouvernement nécessitent une planification stratégique à cinq ans qui permettrait notamment de préciser le positionnement du GIP ACYMA vis-à-vis des autres acteurs de la cybersécurité, les objectifs à atteindre et les ressources qui devraient lui être consacrées.

À plus court terme, l'installation du groupement au sein du cyber campus de La Défense, un instant envisagée avant d'être partiellement abandonnée, ne présente que peu d'intérêt pour l'ensemble de son activité en dehors des nécessaires échanges avec la communauté cyber sur la construction d'un observatoire de la menace, demandée par tous les acteurs. En revanche, le positionnement stratégique de cet observatoire de la menace cyber, comme son fonctionnement et son pilotage doivent faire l'objet d'une réflexion conjointe entre l'ANSSI, le ministère de l'intérieur, le ministère de la justice et le groupement.

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.

RECOMMANDATIONS

Recommandation n° 1 (SGG, SGDSN, ANSSI, GIP) : Renforcer la notoriété du GIP ACYMA auprès des différents publics cibles, notamment les jeunes, les TPE et les PME.

Recommandation n° 2 (ministère de l'intérieur, ministère de la justice, GIP) : Densifier les liens entre tous les acteurs étatiques du « continuum cybermalveillance ».

Recommandation n° 3 (GIP) : Renforcer la gestion administrative de la structure de direction du groupement**.**

Recommandation n° 4 (GIP) : Intégrer la valorisation du personnel mis à disposition dans les comptes financiers afin d'évaluer le coût réel de la masse salariale du GIP ACYMA.

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.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.

Recommandation n° 7 (SGG, SGDSN, ministère de l'intérieur, ministère de la justice, ANSSI, GIP) : Mettre en place l'observatoire de la menace cyber, en fixer les objectifs, la répartition des responsabilités et les modalités de fonctionnement.

INTRODUCTION

La cybercriminalité est un phénomène en croissance exponentielle marqué au cours des derniers mois par la prolifération des escroqueries numériques et des attaques par rançongiciel[1]. Le recours systématisé au télétravail et l'augmentation de l'activité du commerce électronique dans les périodes de confinement ont en outre accentué cette tendance[2]. De plus, toutes personnes physiques, juridiques ou morales peuvent désormais en être victimes, avec des degrés d'exposition variables, qu'il s'agisse du simple individu, des collectivités locales ou territoriales, des organismes de service public, des entreprises petites, moyennes et grandes (TPE/PME/ETI), des grands groupes industriels, OSE[3] ou OIV[4], ou des administrations centrales.

Face à cette menace, et en complément de l'action de l'agence nationale de la sécurité des systèmes d'information (ANSSI), un concept d'assistance aux victimes d'actes de cybermalveillance (ACYMA) a été incubé en 2016 au sein de l'ANSSI. Il s'est matérialisé par un groupement d'intérêt public (GIP) créé juridiquement en 2017[5], et dont l'action, aujourd'hui, paraît non seulement pertinente, mais devrait logiquement s'étendre et s'accroître à l'aune de la croissance prévisible des actes de cybermalveillance.

Trois ans après sa création, le GIP ACYMA a atteint un premier palier dans sa montée en puissance : il regroupe 53 membres, anime la plateforme *cybermalveillance.gouv.fr* et dispose, au 31 décembre 2021, d'un réseau de 1 235 prestataires référencés sur le territoire national. L'organisme se trouve aujourd'hui à la convergence de trois lignes de forces (prévention, assistance, observatoire) qui structurent inégalement son activité et, de fait, justifient l'attention à porter à l'évolution de ses missions, de son organisation, de ses moyens et de son fonctionnement à court et moyen termes.

Le présent rapport analyse dans un premier temps le contexte d'évolution de la menace, la pertinence de la création du groupement et sa gouvernance (1), avant d'aborder l'analyse de sa situation financière, faisant apparaître de nombreux points de fragilité qui nécessiteront des ajustements dans son activité ou dans son financement (2). Enfin, la poursuite du développement du groupement, sa perspective stratégique et l'évolution de son modèle économique soulèvent des questions importantes pour son avenir au sein de la communauté cyber (3).

---

[1] Dispositif malveillant impliquant le chiffrement des données présentes sur l'équipement numérique de la victime en vue d'en obtenir une rançon.
[2] L'impact économique de la cybercriminalité était évalué à 600 milliards de dollars des États-Unis, soit 0,8 % du PIB mondial et 14 % du chiffre d'affaires 2016 de l'économie de l'internet par le rapport 2020 du centre pour les études stratégiques et internationales (*Center for Strategic and International Studies* – CSIS) et de l'éditeur de logiciels de cyberprotection McAfee.
[3] Opérateur de services essentiels tel que défini dans le décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.
[4] Opérateur d'importance vitale, tel que défini par l'article 22 de la loi de programmation militaire n° 2013-1168 du 18 décembre 2013.
[5] Le GIP ACYMA a été créé par arrêté du 3 mars 2017 portant approbation de la convention constitutive du groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance.

1 UNE CRÉATION PERTINENTE FACE À UNE MENACE EN TRÈS FORTE CROISSANCE.

Face à l'ampleur de la menace cyber et devant la recrudescence de la cybercriminalité, le groupement d'intérêt public « assistance aux victimes d'actes de cybermalveillance (ACYMA) » trouve toute sa pertinence dans un vaste champ d'action où nombre d'acteurs sont concernés, au plan national comme au niveau international. Dans ce contexte, associant puissance publique, acteurs privés et collectivités, le lien fort du GIP avec l'État paraît nécessaire à ce stade de sa montée en puissance.

1.1 Un contexte qui confirme le besoin d'une « assistance aux victimes d'actes de cybermalveillance (ACYMA) »

La cybermalveillance, partie intégrante de la cybercriminalité, reste insuffisamment et non officiellement définie alors que les termes liés au domaine cyber sont définis[6] et ont été repris dans les différentes études et rapport sur le sujet de la transformation numérique et ses conséquences. En revanche, les actes de cybermalveillance sont désormais bien identifiés, de plus en plus suivis et exploités, pour les plus significatifs d'entre eux, en termes d'enquêtes et de poursuites judiciaires au niveau national comme au niveau européen.

1.1.1 La cybercriminalité : une menace très diversifiée en augmentation constante

1.1.1.1 Une menace déjà bien identifiée

La police nationale considère deux blocs au sein de la cybercriminalité[7] : d'une part les atteintes aux systèmes de traitement et d'analyse des données (STAD) qui relèvent d'attaques cyber, et, d'autre part, les infractions liées à l'utilisation des nouvelles technologies de l'information et de la communication (NTIC) qui relèvent d'escroqueries de plus ou moins grande ampleur avec de possibles ramifications internationales.

---

[6] Voir annexe n°2.

[7] Selon la direction centrale de la police judiciaire (DCPJ) et plus particulièrement sa sous-direction de la lutte contre la cybercriminalité (SDLC).
État de la menace liée du numérique en 2019 – La réponse du ministère de l'intérieur, rapport N°3 – mai 2019, Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces. *N :* la Délégation ministérielle aux partenariats, aux stratégies et aux innovations de sécurité (DPSIS) a été créée par décret N°2020-1126 du 11 septembre 2020, en fusionnant le délégué ministériel aux industries de sécurité et à la lutte contre les cyber-menaces (DMISC) et la délégation aux coopération de sécurité (DCS).

Comme le note un rapport de l'Assemblée nationale en 2018, les cyberattaques ne relèvent plus de la science-fiction[8]. Elles font désormais partie intégrantes des modes d'actions d'individus ou de groupes criminels, voire de structures étatiques, visant à déstabiliser un pays, bloquer un secteur économique, exercer des pressions sur des personnes ou des systèmes politiques, manipuler des opinions. Elles peuvent aller jusqu'à des attaques à caractère terroriste dont la France n'a jusqu'ici pas eu à subir, selon le directeur général de l'ANSSI, de tentative ayant eu un impact significatif. Ainsi, l'exemple de la cyberattaque subie par l'Ukraine en 2017[9] a provoqué des perturbations majeures dans de nombreux secteurs économiques, y compris hors d'Ukraine. En mai de la même année, le rançongiciel *WannaCry* était parvenu à infecter plus de 300 000 ordinateurs, dans 150 pays. Victime de cette attaque, le service national de santé britannique (*National Health Service* – NHS) avait été durement touché et le fonctionnement de certains services (organisation du système d'ambulances et d'opérations chirurgicales) gravement affecté[10].

Les actes de cybermalveillance sont d'une ampleur moindre mais extrêmement diversifiés, tout en restant traumatisants pour la « victime[11] » entraînant parfois des dommages financiers. Ils font partie du bas du spectre des menaces cyber ; certaines définitions « grand public » vulgarisent la cybermalveillance comme « *une activité englobant toutes les arnaques et autres expériences malhonnêtes qu'un individu peut rencontrer en naviguant sur Internet.* »[12] Cependant, la progression constante du taux de pénétration de l'internet avec plus de 88 % de couverture de la population, conjuguée au développement des réseaux sociaux et à l'utilisation du *smartphone* comme plateforme multi-usage, augmentent mécaniquement à la fois le risque d'être touché par un acte de cybermalveillance et le nombre de cibles potentielles pour les cybercriminels. C'est pourquoi le GIP donne une acception plus large à la cybermalveillance en la définissant comme *« l'ensemble des actes susceptibles de constituer une infraction et commis par l'intermédiaire ou à l'encontre de systèmes numériques. »*

Dans un document[13] de mai 2019, le ministère de l'intérieur évalue les grandes tendances de cybermenaces, avec une année 2017 marquée par des campagnes de rançongiciels qui persistent en 2018. Touchant de nombreuses entreprises françaises, ces attaques ciblent davantage les grandes entreprises ayant une capacité de payer des sommes élevées en échange de la récupération des données volées ou bloquées. L'évaluation du coût de la cybercriminalité reste complexe à établir. Le ministère de l'intérieur estime le coût d'une violation de sécurité pour une entreprise de taille moyenne à plusieurs centaines de milliers d'euros en moyenne. Le préjudice moyen d'un détournement de données pour chaque entreprise victime est évalué à plusieurs millions d'euros, incluant les pertes d'exploitation liées.

---

[8] *« Ce qui pouvait relever hier encore de la science-fiction ou, du moins, de scénarios catastrophes dont on peinait à envisager le caractère réalisable à un horizon prévisible apparaît dorénavant comme une possibilité sérieuse, comme une menace tangible et comme une éventualité stratégique à prendre en considération en termes de doctrine militaire, de conduite des opérations et, plus globalement, d'organisation de la protection et de la résilience de l'ensemble de la société. »* – Rapport d'information de l'Assemblée nationale N° 1141, du 4 juillet 2018, relatif à la cyberdéfense.

[9] Voir annexe n° 4.

[10] Rapport d'information *sur la cyberdéfense*, 4 juillet 2018, Assemblée nationale - commission de de la défense nationale et des forces armées.

[11] Au sens non juridique du terme (voir paragraphe. 1.2.2.2).

[12] *Source : Bonnes pratiques pour se prémunir contre la cybermalveillance / Cybermalveillance : prévention et recommandations / Sécurité numérique / Sécurité / Service Public Entreprises- Monaco (gouv.mc)*

[13] Rapport n°3 du ministère de l'intérieur sur l'état de la menace liée au numérique en 2019.

Les différents types de virus informatiques

Trois types de virus sont susceptibles d'infecter un ordinateur ou un système d'information.

Le **virus informatique classique ou « ver »** infecte un ordinateur par l'intermédiaire d'un périphérique externe (clé USB, CD ou DVD, disque dur externe, etc.) ou d'un fichier attaché à un message e-mail ou téléchargé à l'insu de l'utilisateur lors d'une connexion internet à un site web ou à un réseau social. Son but est alors de se répandre à l'intérieur du système de fichier ou du réseau local de l'ordinateur infecté en vue de collecter des informations ou simplement de se diffuser à d'autres postes utilisateurs.

Le **maliciel** (*malware* en anglais) est un virus dont l'objet est de compromettre un ordinateur, soit pour en effacer ou pirater les données, soit pour recueillir des données compromettantes ou informations sur les moyens de paiement de l'utilisateur (numéro de carte ou de compte bancaires), soit encore pour crypter le support physique de stockage principal (disque dur ou SSD) de l'ordinateur infecté afin de mener un chantage auprès de l'utilisateur (rançongiciel). Il peut également envoyer des annonces publicitaires non désirées (*« adware »*) sur le poste infecté. Il peut aussi utiliser le poste infecté pour exécuter des programmes malveillants (*« rootkit »*) destinés à provoquer des attaques en déni de service sur des sites (Ddos), forer des cryptomonnaies ou envoyer des messages commerciaux non sollicités massifs (SPAM) par l'intermédiaire de la propre messagerie de l'ordinateur infecté. On parle alors d'« ordinateur zombie », pouvant faire l'objet d'un commerce sur le « Darkweb » (*« botnet »*).

Le **logiciel espion** (ou *spyware* en anglais) a pour unique but la collecte d'informations sensibles sur le poste utilisateur, qu'il s'agisse de celles stockées dans les fichiers de l'ordinateur infecté ou de celles saisies par l'utilisateur, généralement à l'aide de son clavier, pour dérober notamment les informations de connexion (identifiants et mots de passe).

Depuis 2018, le *spearphishing* et le *cryptojacking* (minage clandestin de cryptomonnaie) sont en nette augmentation. De même, les *malwares* bancaires sont en plein essor, notamment sur les *smartphones*, et les attaques de distributeurs bancaires s'intensifient et se diversifient. Tout un système facilitant la mise en œuvre d'attaques cyber par des individus ou des groupes criminels est désormais bien en place, mettant en lumière la notion de « *crime-as-a-service*[14] *(CAAS)* ». Maliciels, plateformes d'exploit, de service ou prestataires d'infrastructures « clés en mains » sont aisément disponibles, particulièrement sur le *darknet*[15].

Ce risque était classé au premier rang des risques d'entreprise identifiés pour 2020 par l'assureur Allianz[16], quelques mois avant l'essor du télétravail et des cyberattaques lié à la pandémie de COVID-19.

[14] Par analogie avec le concept de *software as service* (logiciel utilisé comme un service), cette caractérisation indique que les cybercriminels peuvent parfois louer toute ou partie des fichiers, logiciels et infrastructures nécessaires à l'accomplissement de leurs forfaits à d'autres groupes criminels spécialisés, en passant généralement par l'intermédiaire de la partie criminelle d'internet (*« dark web »*) et en réglant ces « prestations » au moyen de crypto-monnaies telles que BitCoin ou Monero.
[15] Voir annexe n°3.
[16] Communiqué de presse du 14 janvier 2020.

1.1.1.2 Une cybercriminalité qui élargit son rayon d'action et diversifie ses points d'application

Les principales tendances de la menace observées en 2019 sont dans la continuité des années précédentes. Selon le GIP ACYMA[17], l'hameçonnage (*phishing*) reste la menace prédominante et se diversifie. Ces attaques touchent aussi bien les particuliers que les professionnels. Autrefois facilement identifiables, elles apparaissent de mieux en mieux réalisées et même les internautes les plus avertis peuvent parfois s'y faire prendre. Les faux remboursements de la sécurité sociale ou des impôts, ou les fausses confirmations de commandes sur Internet restent dans le peloton de tête des vagues régulières qui ciblent les particuliers.

Du côté des professionnels, les arnaques à la mise en conformité avec le règlement général de protection des données (RGPD)[18] ou à la fermeture d'un nom de domaine font des victimes notamment sur les plus petites structures. Les grands acteurs industriels, comme de petites entreprises, des collectivités de toutes tailles, des hôpitaux, sont également la cible de rançongiciels (*ransomware*) qui gagnent en sophistication, avec toutes les conséquences, potentiellement graves, sur leurs activités. En 2019, les rançongiciels ont représenté 8 % des recherches d'assistance par les entreprises et collectivités sur la plateforme cybermalveillance.

Le rançongiciel cible désormais plus les entreprises

Selon le ministère de l'intérieur[19], en 2018, 80 % des entreprises ont constaté au moins une cyberattaque et plus de 10 pour 32 % d'entre-elles, soit respectivement un et quatre points de plus qu'en 2017, les entreprises les moins bien protégées donc les plus vulnérables, étant de plus en plus ciblées. Si depuis 2017, les entreprises sont la cible privilégiée d'attaques au rançongiciel, la baisse de 20 % des infections par rançongiciel en 2019 dans le monde a été compensée, selon l'éditeur de logiciels de sécurité américain Symantec[20], par une hausse de 12 % des attaques à l'encontre des entreprises, en ciblant leurs salariés.

Dans son rapport d'état de la menace rançongicielle en France en 2020[21], l'agence nationale de la sécurité des systèmes d'information (ANSSI) pointe une hausse des signalements d'attaque de 255 % par rapport à 2019. En 2020, l'ANSSI estime que le nombre de rançongiciels a quadruplé. Plus d'une entreprise sur deux aurait connu une cyberattaque en 2020 selon le club des experts de la sécurité de l'information et du numérique (CESIN)[22].

---

[17] Rapport d'activité 2019 du GIP ACYMA.

[18] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. L'arnaque au RGPD consiste en un message mettant en demeure de mise en conformité RGPD à fins d'hameçonnage.

[19] *« État de la menace liée au numérique en 2019 », rapport n°3*, ministère de l'intérieur.

[20] *« Internet Security Threat Report 2019 », février 2019.*

[21] *« Attaques par rançongiciels, tous concernés : comment les anticiper et réagir en cas d'incident ? »*, ANSSI, août 2020.

[22] Créé en juillet 2012, avec des objectifs de professionnalisation, de promotion et de partage autour de la sécurité de l'information et du numérique, le CESIN est un lieu d'échange, de partage de connaissances et d'expériences. Il permet la coopération entre experts de la sécurité de l'information et du numérique et entre ces experts et les pouvoirs publics. Il participe à des démarches nationales et est force de proposition sur des textes réglementaires,

Nota : tous ces chiffres de la cybersécurité sont à prendre avec précaution et ne reflètent pas l'intégralité des attaques, toutes les entreprises ne déclarant pas aux autorités judiciaires les préjudices dont elles ont été victimes.

L'hameçonnage[23] sur les réseaux sociaux tend aussi à se développer, car il permet souvent de contourner la protection contre les maliciels mise en place par les opérateurs de messagerie sur leurs passerelles. L'hameçonnage représente en 2019 la première menace pour les entreprises avec 23 % des recherches d'assistance et la troisième menace pour les particuliers avec 13 % des recherches d'assistance (voir *infra*).

Les arnaques au faux support technique continuent de se développer largement. Identifiée par le dispositif *cybermalveillance* fin 2017 et étendue en 2018, cette catégorie d'attaque ne cesse de gagner en sophistication, avec des discours de cybercriminels très crédibles et étayés de documents d'apparence officielle (factures, contrats).

Avec une première alerte lancée en 2018 par le GIP ACYMA, le chantage à la webcam est un phénomène qui a explosé en 2019. Il s'agit le plus souvent d'une simple arnaque[24] à la faible dimension technologique.

1.1.1.3 Une situation cybercriminelle qui s'installe dans la durée en 2020

Tous les rapports consultés ainsi que le rapport d'activité 2020 du GIP témoignent d'une intensification des activités cybercriminelles qui se sont développées de manière contextualisée ou opportuniste. L'hameçonnage sous toutes ses formes reste l'un des principaux vecteurs à l'origine de multiples attaques informatiques, recourant de plus en plus aux SMS. Le piratage de comptes en ligne représente la deuxième menace constatée par la plateforme, tous publics confondus, particuliers comme professionnels, avec des effets parfois dévastateurs pour les victimes. Les arnaques au faux support technique conservent leur intensité, avec des modes opératoires qui continuent d'évoluer. Enfin, les rançongiciels sont toujours la première cause des recherches d'assistance des publics professionnels des secteurs privés et publics (voir *infra*), avec une intensification sans précédent en 2020 et des conséquences souvent désastreuses.

Les phases de confinement imposées par la gestion de l'épidémie de Covid-19 en mars 2020 et en octobre 2020, ont permis à la cybercriminalité de se développer et de tirer profit de la systématisation du télétravail et de l'explosion du commerce en ligne, en exploitant les failles structurelles de sécurité sur les systèmes d'informations des organismes ou entreprises (notamment les TPE/PME/ETI) et la crédulité des bénéficiaires des services en ligne.

guides et autres référentiels. Le CESIN compte plus de 600 membres issus de tous les secteurs d'activité économique et de l'administration.

[23] Par exemple, de faux bons d'achats pour des grandes surfaces, des places gratuites dans des parcs d'attractions ou des billets gratuits de compagnies aériennes.

[24] Aucun cas de piratage réel n'a été rapporté en 2019 à la plateforme *cybermalveillance.gouv.fr*
Suite à la mise en place sur cette plateforme d'une lettre plainte permettant de signaler ce type d'arnaque aux autorités judiciaires, deux arrestations ont pu avoir lieu en France en septembre et décembre 2019.

L'exemple de trois attaques frappant des PME

En mai 2021 une PME du Sud-Ouest de quatre personnes spécialisée dans la réparation d'électroménager est frappée par un rançongiciel. Deux semaines après l'attaque, l'ensemble de ses données et sauvegardes restent inaccessibles (fichiers clients, agenda d'intervention, facturation) et l'entreprise reste paralysée. Même s'il ne souhaitait pas s'y résoudre, le chef d'entreprise envisage de payer la rançon au risque de devoir déposer le bilan de sa PME.

À l'été 2020, une PME d'Auvergne de 40 salariés spécialisés dans les salaisons s'aperçoit que des virements suspects ont été réalisés pour un montant de 110 000 €. Un escroc avait usurpé par messagerie l'identité du chef d'entreprise pour manipuler sa comptable en lui faisant croire à une opération financière confidentielle. Malgré l'action de l'entreprise et des forces de l'ordre, seule la moitié des fonds a pu être récupérée.

Au printemps 2020, une entreprise d'Île de France de 2 500 personnes spécialisée dans les fournitures de bureau détecte que son site internet de vente en ligne a été piraté par des cybercriminels. Ceux-ci ont mis en place un système de duplication des informations des cartes bancaires au moment d'un achat sur leur site web. La crédibilité de l'entreprise vis-à-vis des clients, partenaires et investisseurs est durablement amoindrie.

Enfin, selon le dossier de presse du gouvernement le 18 février 2021 présentant la stratégie française de cybersécurité et annonçant la création d'un campus cyber, la menace s'exerce actuellement autour de trois tendances spécifiques :

- le développement du rançongiciel[25] ;
- la professionnalisation des cybercriminels et l'industrialisation de la menace ;
- une vulnérabilité particulière des organismes publics et collectivités, notamment ceux de petite taille.

1.1.2 Une réponse française à la cybercriminalité : l'ANSSI, de la protection de l'État en 2009 à celle du citoyen à partir de 2015

1.1.2.1 Une prise de conscience des enjeux de cybersécurité par le haut

Le Livre blanc sur la défense et la sécurité nationale de 2008 intègre la menace cyber comme « *une menace majeure les plus probables des 15 prochaines années* ». Pour y faire face, l'État doit se doter d'une capacité de prévention et de réaction aux attaques informatiques, en faisant une priorité majeure du dispositif étatique de sécurité nationale[26]. Une agence nationale a été créée dès 2009 – l'agence nationale de la sécurité des systèmes d'information (ANSSI)[27] –

[25] Entre 2019 et 2020, le nombre d'attaques traitées par l'ANSSI aurait été pratiquement multiplié par quatre, passant de 54 à 192.
[26] La défense des systèmes d'information doit disposer d'une capacité de détection précoces des attaques et d'une organisation propre à contrer les attaques les plus subtiles et massives, de même qu'une capacité de prévention et un réservoir de compétences au profit des administrations et des opérateurs d'infrastructures vitales (*source LBDSN 2008)*.
[27] Décret n° 2009-834 du 7 juillet 2009, créant l'ANSSI en tant que service à compétence nationale (SCN).

pour traiter les attaques informatiques et protéger les systèmes d'information de l'État et des infrastructures critiques, avec comme objectif la mise en place d'une stratégie nationale en matière de sécurité des systèmes d'information (SSI), d'un comité stratégique de la SSI et d'un observatoire zonal de la SSI dans chaque zone de défense pour relayer au niveau régional et local les mesures prises au niveau national pour améliorer la SSI.

Cette priorité nationale se décline en textes fondateurs pour la sécurité des systèmes d'information, avec une première stratégie de cybersécurité de la France élaborée début 2010[28] et publiée début 2011, accompagnée en 2014 d'une politique de sécurité des systèmes d'information de l'État (PSSIE) qui s'applique à toutes les administrations[29] ; puis une stratégie nationale pour la sécurité du numérique en octobre 2015, présentée comme « *une réponse collective pour la sécurité des systèmes d'information* », et enfin, en février 2021, une stratégie nationale pour la cybersécurité dont la mise en œuvre prévoit un milliard d'euros dont plus de 700 millions de fonds publics.

Elle se traduit également en ressources dans la loi de programmation militaire de 2014-2019[30], qui fait du cyberespace une priorité stratégique, dont la cyberdéfense, notamment en termes de recrutement [31], confirmée dans la nouvelle loi de programmation 2019-2025[32].

Cette prise de conscience des risques et des enjeux de cybersécurité sur tout le spectre des menaces, par l'ensemble des acteurs étatiques et privés, conjuguée à une mobilisation de ressources très importantes, doit désormais se traduire par des objectifs de performance précis et une coordination à la fois nationale et locale des actions à entreprendre pour répondre aux ambitions de la nouvelle stratégie.

1.1.2.2 La lutte contre les actes de cybermalveillance : une cybersécurité pour tous avec une approche pas le bas du spectre des cibles potentielles

La stratégie de cybersécurité française évolue en 2015 avec la prise en compte, au-delà des seuls opérateurs d'intérêt vital (OIV) et opérateurs de services essentiels (OSE), de toutes les cibles potentielles de la cybercriminalité. En effet, cette stratégie nationale prévoyait la mise en place *« d'un dispositif d'assistance aux victimes de cybermalveillance qui apportera une réponse technique et judiciaire »* aux actes de cybermalveillance. Elle disposait qu'*« afin que le cyberespace reste un espace de confiance pour les entreprises de toutes tailles et les*

[28] Suite à la découverte d'une attaque informatique à des fins d'espionnage contre les ministères de l'économie et des finances.
[29] Entré en vigueur le 29 août 2014, elle s'applique aux ministères, établissements publics sous tutelle d'un ministère, services déconcentrés de l'État et autorités administratives indépendantes.
[30] Loi n° 2013-1168 du 18 décembre 2013 – Article 22 qui prévoit l'adoption de mesures de renforcement de la sécurité des opérateurs d'importance vitale, et de nouvelles prérogatives au Premier ministre.
[31] « *L'objectif RH de l'ANSSI a été fixé à 500 ETP, le programme 178 pourra créer 350 postes supplémentaires consacrés à la cyberdéfense et cyberprotection, la DGA pourra étoffer ses équipes SSI avec 200 postes nouveaux (pour arriver à un peu plus de 400 personnes). Un PEM SSI est doté de 350 M€ sur la période LPM. Les programmes d'étude en amont disposeront de 180 M€ (soit 30 M€ par an)*. »
[32] L'article 34 de la loi du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 (LPM) complète les missions de l'ANSSI en précisant la mise en œuvre des dispositifs de détection lors d'événements susceptibles d'affecter la sécurité des systèmes d'information de l'État, des autorités publiques, et d'opérateurs publics et privés, ainsi que le recueil d'informations techniques relatives à des incidents et l'accompagnement pour y répondre.

particuliers, des mesures de protection et de réaction seront adoptées. La protection passera par une vigilance accrue des pouvoirs publics sur l'utilisation des données personnelles et par le développement d'une offre de produits de sécurité numérique adaptée au grand public. »

Devant la recrudescence des actes de cybermalveillance (voir *supra*), et en particulier les rançongiciels, un projet de dispositif d'assistance aux victimes a donc été développé au sein de l'ANSSI en 2016 visant à sensibiliser un large public (particuliers, entreprises, administrations publiques, collectivités territoriales, communes, monde associatif, etc.) pour prévenir le risque cyber, à apporter un soutien technique aux personnes, organismes ou entreprises ayant subi une attaque ou un préjudice, et à observer l'évolution de la menace pour mieux s'en protéger.

Un groupement d'intérêt public (GIP) dénommé « assistance aux victimes d'actes de cybermalveillance (ACYMA) » est créé le 3 mars 2017. Dispositif original porté par un partenariat public-privé, le GIP ACYMA regroupe des acteurs étatiques tels que l'ANSSI qui relève des services du Premier ministre, le ministère de l'intérieur, le ministère de la justice, le ministère de l'économie et des finances, le secrétariat d'État en charge du numérique et le ministère des armées. Il rassemble également de nombreux acteurs de la société civile comme des associations de consommateurs ou d'aides aux victimes, des représentations professionnelles de type fédération ou syndicat, des assureurs, des opérateurs, des éditeurs[33]… Son activité ne cesse de croître depuis sa création (voir *infra*), *via* la plateforme *Cybermalveillance.gouv.fr* mise en œuvre en octobre 2017.

Les dates clés de la création du GIP ACYMA

18 juin 2015 : Annonce par le Premier ministre de la mise en place d'un dispositif national d'assistance aux victimes d'actes de cybermalveillance lors de sa présentation de la stratégie numérique du gouvernement.

16 octobre 2015 : Confirmation par le Premier ministre de la mise en place d'un dispositif national d'assistance aux victimes d'actes de cybermalveillance lors de son intervention relative à la stratégie nationale pour la sécurité du numérique.

2016/2017 : Incubation du projet par l'ANSSI en copilotage avec le ministère de l'intérieur, et le soutien des ministères de la justice, de l'économie et des finances, ainsi que le secrétariat d'État en charge du numérique.

Avril 2016 : Mise en place d'une équipe de préfiguration au sein de l'ANSSI en co-pilotage avec le ministère de l'intérieur.

3 mars 2017 : Arrêté de constitution du groupement d'intérêt public « Action contre la Cybermalveillance (GIP ACYMA) » afin de réunir autour du projet commun les acteurs publics et privés de la cybersécurité ; mise à jour par un arrêté du 13 novembre 2020 ainsi qu'un arrêté du 24 décembre 2020, portant approbation des modifications de la convention constitutive du groupement d'intérêt public dénommé « groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance ».

17 octobre 2017 : Généralisation du dispositif sur l'ensemble du territoire national après une phase d'expérimentation de quatre mois sur la région des Hauts-de-France, et lancement national de la plateforme Cybermalveillance.gouv.fr

Source : GIP ACYMA

[33] Le GIP compte, en novembre 2021, 53 membres publics et privés.

1.1.3 Une prise en compte de la menace au niveau international

La lutte contre la cybercriminalité et la cybermalveillance est, par essence, internationale puisque les faits commis peuvent s'exercer sur ou à partir de territoires ou d'États complètement différents et que les victimes et les auteurs d'actes de cybermalveillance sont disséminés à travers le monde entier.

1.1.3.1 Une coopération juridique internationale en nette progression

La coopération juridique internationale s'organise autour de trois grands instruments juridiques, portés par le Conseil de l'Europe (COE) et par l'Union européenne.

La convention de Budapest sur la cybercriminalité[34], a pour ambition d'harmoniser les législations nationales en matière d'incrimination et de sanctions pénales pour une liste de délits (voir encadré) et de renforcer les législations pénales en matière d'investigation et de preuve. Elle prévoit également les conditions d'assistance dans lesquelles les différents acteurs nationaux peuvent coopérer dans le cas – fréquent – d'incriminations transnationales.

Elle dépasse très largement le cadre des seuls États-membres du Conseil de l'Europe puisque les États-Unis ou le Sri Lanka notamment en sont signataires. La Fédération de Russie est le seul État-membre du Conseil de l'Europe à ne pas avoir signé la convention. Elle a présenté au comité spécial de l'ONU en juillet 2021, sans beaucoup de succès, un projet alternatif de convention mondiale contre la cybercriminalité et l'utilisation criminelle de la cryptomonnaie.

Convention de Budapest

Cette convention, portée par le Conseil de l'Europe et signée par les États-membres mais également par l'Afrique du Sud, le Canada, le Japon et les États-Unis en novembre 2001, constitue l'un des principaux instruments de la lutte internationale contre la cybercriminalité.

Elle vise à mettre en place une politique pénale commune par les parties, destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et l'amélioration de la coopération internationale.

Neuf infractions principales sont mentionnées par la convention, parmi lesquelles :

- l'accès illégal ;
- l'interception illégale ;
- l'interférence de données ;
- l'interférence de système ;
- l'utilisation abusive d'appareils ;
- la contrefaçon informatique ;
- la fraude informatique ;
- les infractions liées à la pédopornographie et les infractions liées à la violation du droit d'auteur et des droits connexes.

[34] Convention de Budapest sur la cybercriminalité.
https://www.coe.int/fr/web/conventions/full-list/-/conventions/rms/090000168008156d

Un protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques a été ajouté en janvier 2003. Un second protocole additionnel relatif au renforcement de la coopération et de la divulgation de preuves électroniques a été adopté par le comité des ministres le 17 novembre 2021.

Au 1er septembre 2021, 66 États (dont 45 des 47 États-membres du Conseil de l'Europe[35]) avaient ratifié la convention.

Elle prévoit notamment la mise en œuvre de mécanismes d'entraide internationale et la possibilité pour les États parties de requérir des informations ou des mesures conservatoires telles que la préservation des données et de leur intégrité auprès de prestataires étrangers (articles 29 et 30 de la convention).

Le deuxième instrument est le règlement général sur la protection des données (RGPD) de l'Union européenne qui renforce et unifie les mécanismes nationaux de protection des données et établit un régime de responsabilité pour les gestionnaires de ces données. Sa particularité est de pouvoir s'appliquer à des acteurs extra-européens.

Enfin, la directive 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 sur la sécurité des réseaux et des systèmes d'information (SRI), dite « directive NIS », transposée en 2018 en droit français[36], permet la mise en place d'un cadre réglementaire visant à renforcer la cybersécurité, en complément de celle des opérateurs d'importance vitale, des opérateurs de services essentiels au fonctionnement de l'économie et de la société et des fournisseurs de services numériques (FSN).

Une agence de l'Union européenne (UE), l'agence européenne chargée de la sécurité des réseaux et de l'information[37], dont le siège est en Grèce, existe depuis 2004[38]. Elle constitue un centre d'expertise pour la cybersécurité en Europe afin d'assister les pouvoirs publics dans l'identification des enjeux et de proposer des solutions techniques pour lutter contre les menaces. Ses missions principales sont de conseiller les institutions de l'UE et les États-membres en matière de cybersécurité et de favoriser l'échange de bonnes pratiques, en mettant notamment en place des partenariats entre le secteur public et le secteur privé, en particulier les entreprises spécialisées dans ce domaine. L'ENISA organise depuis 2010 un exercice bisannuel dénommé *Cyber Europe*, qui permet aux États membres de tester leur collaboration en cas de crise.

1.1.3.2 Le modèle du GIP est un modèle original, sans équivalent au plan européen

Les missions de mise en relation des victimes avec les prestataires chargés de la remédiation et leur sélection distinguent le GIP par rapport aux modèles retenus par d'autres pays européens.

[35] L'Irlande a signé mais pas ratifié et la Fédération de Russie n'a pas signé le traité.
[36] Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.
[37] ENISA selon son acronyme en anglais.
[38] Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'agence européenne chargée de la sécurité des réseaux et de l'information.

1.1.3.2.1 L'exemple britannique d'une réponse centralisée visant tous les publics

La Grande-Bretagne a fait le choix, en 2016, au travers de sa stratégie nationale de cybersécurité 2016-2021[39] de confier la mission de dissuader et de protéger des attaques les trois principaux publics (individus, organisations gouvernementales, entreprises) à un organisme unique, le *National Cyber Security Center* (NCSC), rattaché au Premier ministre (*cabinet office*).

À l'occasion du rapport de 2016 sur le contrôle de la cyber-hygiène et des failles de cybersécurité[40], le gouvernement britannique notait que *« l'an passé, le coût moyen des attaques réussies était de 36 500 livres pour les grandes entreprises. Le coût moyen pour les PME était de 3 100 livres. 65 % des grandes organisations avaient souffert d'une attaque informatique pendant l'année et 25 % pendant au moins un mois. Environ sept sur dix de ces attaques avaient impliqué des virus informatiques, des logiciels espions ou des maliciels qui auraient pu être contenus en utilisant le dispositif gouvernemental de fondamentaux cyber* (Government's Cyber Essentials Scheme) ».

1.1.3.2.2 La Belgique possède une plateforme d'échanges entre professionnels de la cybersécurité, administrations et entreprises

La *Cyber Security Coalition* (sic) est une communauté regroupant des acteurs du monde universitaire, des services publics et des entreprises privées *« afin qu'ils unissent leurs forces dans leur combat contre la cybercriminalité »*. La Belgique dispose d'une plateforme d'échanges entre professionnels de la cybersécurité, administrations et entreprises, mais qui ne ressemble en rien à une structure s'adressant au grand public Il s'agit plus d'un forum destiné au partage d'expérience (connaissances, meilleures pratiques, menaces et opportunités) et à la collaboration opérationnelle entre pairs. Il a également vocation à diffuser des recommandations pour des politiques et des lignes directrices plus efficaces et à renforcer la conscience de la menace par les citoyens et les organisations par des campagnes de sensibilisation.

Cette plateforme d'échanges ne propose pas, pour autant, de service de diagnostic ou de remédiation par mise en rapport avec des tiers qualifiés comme le fait le GIP Acyma. En réponse aux observations provisoires de la Cour, le GIP ACYMA indique qu'il échange avec le centre pour la cybersécurité Belgique (CCB), autorité nationale en charge de la cybersécurité en Belgique, afin que ce dernier puisse disposer des outils techniques développés par le GIP (plateforme et outils associés), sur le modèle du logiciel libre, pour proposer les mêmes services, et en particulier la mise en relation avec des prestataires de proximité pour les particuliers, entreprises et collectivités belges.

[39] National Cyber Security Strategy 2016-2021 (publishing.service.gov.uk).
[40] *2016 Government Cyber Health Check and Cyber Security Breaches Survey*.

1.2 Un champ d'action large et de nombreux acteurs impliqués

Le champ d'action du GIP est extrêmement large et la dynamique imprimée dès la création de *Cybermalveillance.gouv.fr* en 2017 a permis de couvrir progressivement le besoin urgent d'assistance aux « victimes », de lancer les premières campagnes d'information du grand public sur les risques cyber et d'amorcer le flux des informations vers les services concernés des ministères de l'intérieur et de la justice.

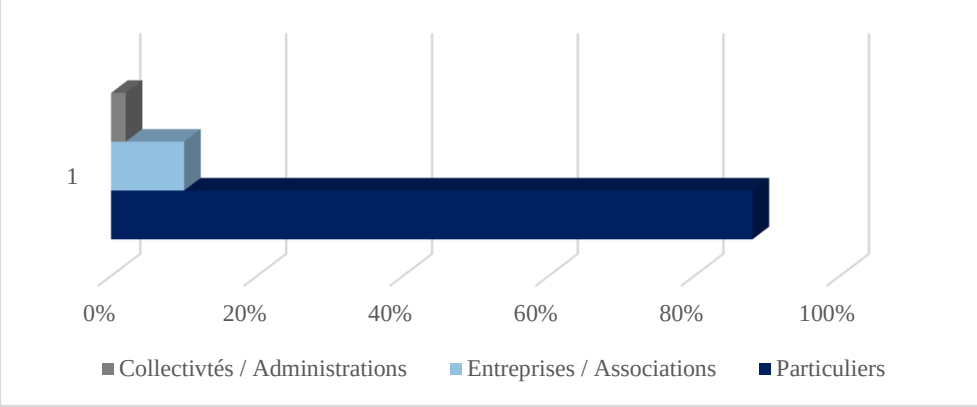
1.2.1 Le GIP ACYMA : un programme réalisé aux deux-tiers

1.2.1.1 Un besoin d'assistance en forte croissance qui s'appuie sur un réseau de professionnels en construction

L'actualité de ces trois dernières années confirme la diffusion de la menace auprès du grand public et d'organismes peu touchés auparavant, composant un ensemble hétérogène de particuliers, de collectivités, de PME-ETI et d'organismes divers (hôpitaux, associations, etc.). Le GIP annonce près de 225 000 victimes assistées depuis le lancement du dispositif *Cybermalveillance.gouv.fr* en 2017.

Dans son rapport d'activité 2019, le GIP fait état d'une demande croissante d'information ou d'assistance ; un besoin qui s'est fortement accru en 2020, se traduisant par une fréquentation de la plateforme *Cybermalveillance.gouv.fr* en augmentation de 155 %, avec 1 235 545 visiteurs. La répartition des victimes par type de publics pour ces recherches a été de 88% pour les particuliers, 10 %, pour les entreprises et associations, et 2 % pour les collectivités et des administrations[41]. Le nombre de recherches de diagnostic et d'assistance en ligne s'élève à près de 105 000, soit une hausse de 16 % par rapport à 2019.

Graphique n° 1 : Répartition 2020 des recherches par types de public



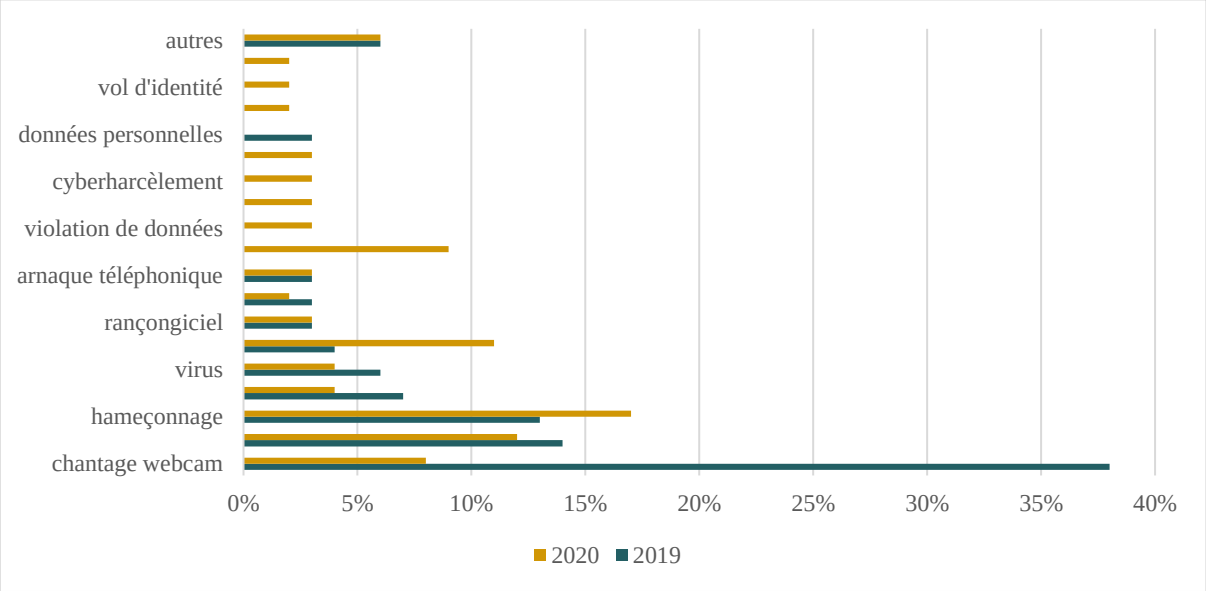
Source : Cour des comptes, d'après les données du GIP ACYMA

[41] Rapport d'activité 2020 du GIP ACYMA.

Les demandes d'assistance émanant des particuliers en 2019 ont principalement porté sur le chantage à la webcam (38 %), suivi du piratage de compte en ligne (14 %) et de l'hameçonnage (13 %) devant les spams (7 %), les virus (6 %) et les arnaques au faux support technique (4 %).

En 2020, la tendance se confirme avec des recherches d'assistance portant principalement sur l'hameçonnage (17 %), suivi du piratage de compte (12 %) et du faux support technique (11 %).

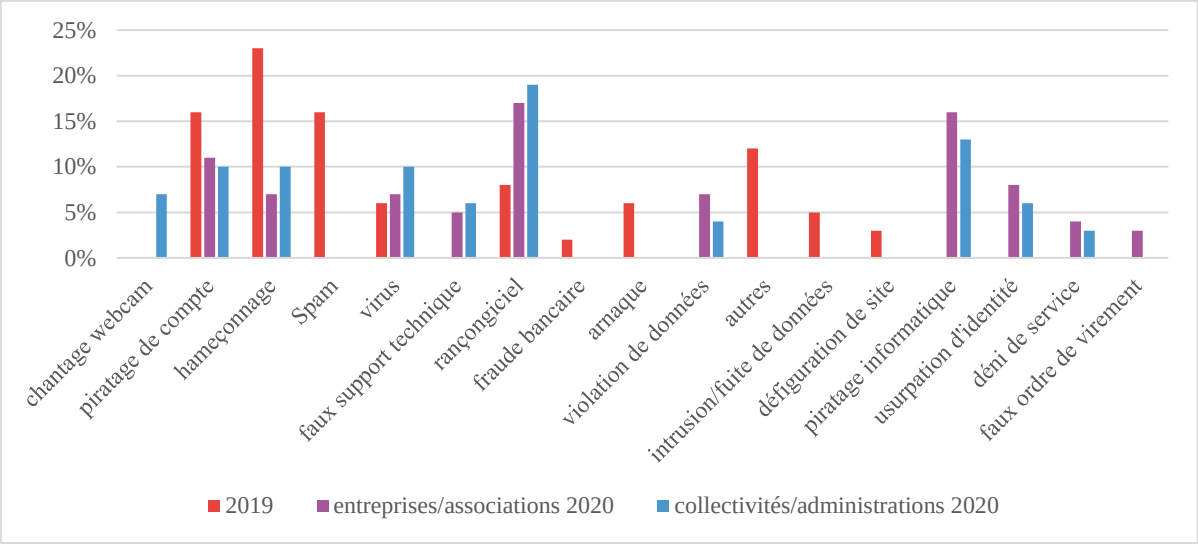
Graphique n° 2 : Recherche d'assistance des particuliers par type de menace



Source : Cour des comptes, d'après les données du GIP ACYMA

Alors que les particuliers représentent en 2020 toujours près de 90 % des publics de la plateforme, le GIP note une augmentation de 20 % des recherches d'assistance provenant de publics professionnels (entreprises, associations, collectivités, administrations). Pour les professionnels (entreprises, collectivités et associations), l'hameçonnage arrive en tête (23 %) des recherches d'assistance en 2019, devant le piratage de compte en ligne (16 %), le spam (16 %), les virus (9 %) et les rançongiciels (8 %). La tendance s'inverse en 2020. Pour les « entreprises et associations » ou les « collectivités et administrations », les rançongiciels ont été la première cause de recherche d'assistance, avec respectivement 17 % et 19 %, progressant de 30 % par rapport à 2019, suivi du piratage informatique (16 % et 13 %) et du piratage de compte.

Graphique n° 3 : Recherche d'assistance des professionnels par type de menace



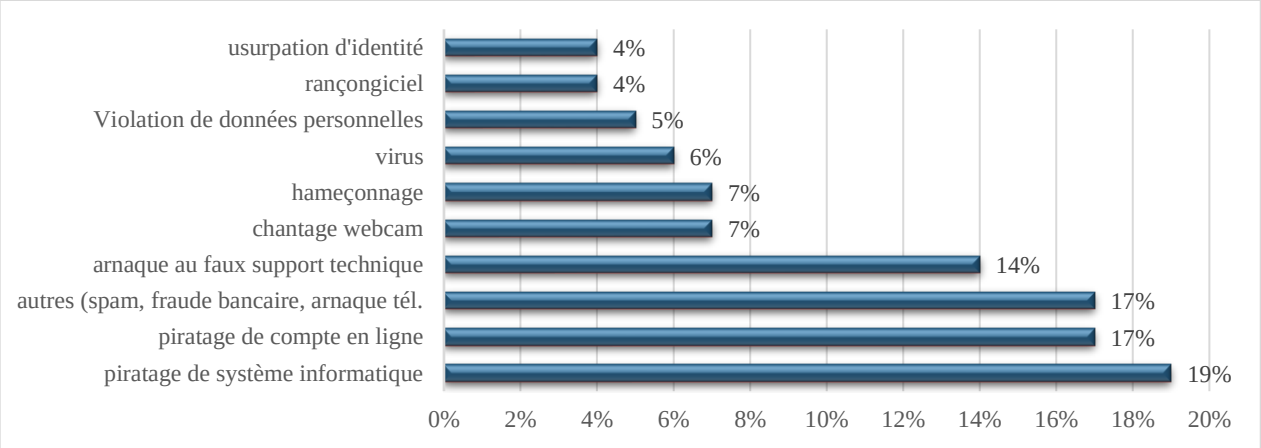
Source : Cour des comptes, d'après les données du GIP ACYMA

Deux facteurs contribuent à la notoriété du GIP :

- un réseau de prestataires professionnels d'assistance aux victimes[42] qui comporte, en 2020, près de 1 000 organismes référencés sur le territoire national[43],pouvant désormais être labellisés *ExpertCyber* depuis début 2020[44] ;
- la plateforme *Cybermalveillance.gouv.fr* qui a été refondue et améliorée en février 2020 pour mieux répondre aux attentes des publics, les assister plus efficacement et mettre à leur disposition des outils de prévention.

[42] Les domaines couverts par ces prestataires sont les applications Web, les objets connectés, les équipements industriels, la téléphonie fixe, la sauvegarde de données, les systèmes d'exploitation.
[43] Avec la mise en place de la nouvelle version de la plateforme début 2020, une campagne de réinscription des prestataires a été lancée avec un contrôle administratif renforcé. Au 31 décembre 2021, 1 235 prestataires sont référencés sur la plateforme *Cybermalveillance.gouv.fr* (*p.m* 1534 prestataires référencés en 2018 et 1633 en 2019).
[44] Annoncé par le GIP ACYMA le 12 décembre 2019, le label *ExpertCyber* est développé par Cybermalveillance.gouv.fr, en partenariat avec les principaux syndicats professionnels du secteur (Fédération EBEN, Cinov Numérique, Syntec Numérique), la Fédération Française de l'Assurance et le soutien de l'AFNOR et lancé début 2020 à l'occasion d'une conférence organisée avec Syntec Numérique. A la date de parution du présent rapport, 139 prestataires sont labellisés *ExperCyber*.

Graphique n° 4 : Demandes de mise en relation avec un professionnel référencé en 2020 (toutes catégories de victimes confondues)



Source : Cour des comptes d'après les données du GIP ACYMA

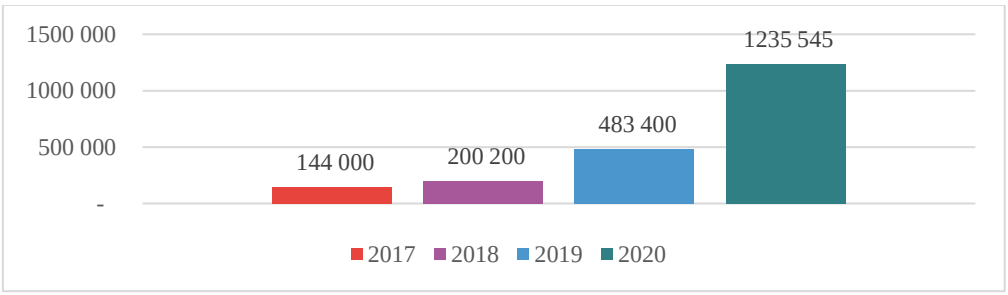
Le GIP complète donc l'offre de l'État en fournissant une réponse technique et pratique à un public hors OIV/OSE au niveau local qui se trouve démuni devant une agression cyber. La force du GIP réside dans sa capacité à faire le lien, via son réseau de partenaires et de prestataires, entre la victime potentielle, les services des ministères de l'intérieur et de la justice, et les sociétés capables d'apporter rapidement une solution au problème rencontré.

Facteur clé de la réussite de la mission du GIP, l'extension de ce réseau doit se poursuivre et son animation amplifiée, notamment dans les régions et sur les territoires à la fois au niveau des acteurs publics, en liaison avec les antennes de l'ANSSI, des entreprises (prioritairement TPE/PME, mais également ETI), et des professionnels de la remédiation des systèmes d'information.

1.2.1.2 Une notoriété de *Cybermalveillance.gouv.fr* à renforcer

Le GIP considère que la sensibilisation est « *la première arme contre les cybermalveillances* ».

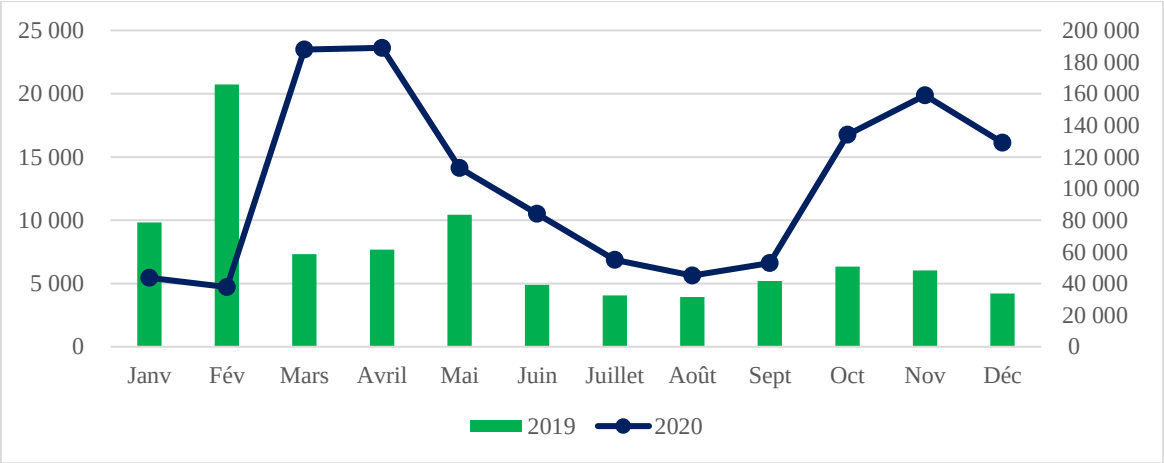
Graphique n° 5 : Fréquentation annuelle de la plateforme *Cybermalveillance.gouv.fr*



Source : Cour des comptes d'après les données du GIP ACYMA

À cet égard, l'effort de communication tous publics produit depuis 2017 est significatif. Il se traduit par une série de produits allant de kits pédagogiques de sensibilisation et de publications sur le site *Cybermalveillance.gour.fr*, à des campagnes d'information sur les réseaux sociaux et dans les médias nationaux. Ainsi, les activités du GIP en 2020 font état de la publication de 260 communications[45], dont 41 alertes, sur les réseaux sociaux. Les articles sur les différentes menaces et sur les moyens d'y faire face ayant recueilli en 2020 près de 650 000 consultations, le GIP considère que la plateforme a informé ou apporté une assistance à plus de 755 000 personnes en 2020, soit une augmentation de plus de 730 % par rapport à 2019.

Graphique n° 6 : Fréquentation mensuelle de la plateforme *Cybermaveillance.gouv.fr*



Source : Cour des comptes, d'après les données du GIP ACYMA

Cette prise de conscience du risque cyber apparaît également dans le 6e baromètre de la sécurité des entreprises de février 2021 du Club de sécurité de l'information français[46], où on relève que « *les entreprises, conscientes de la recrudescence de la menace rançongiciels en 2020 renforcent la sensibilisation des utilisateurs (83 %) à ce type d'attaque.* »

Or, il apparaît à travers une étude menée en juillet 2020 par le GIP en partenariat avec l'institut national de la consommation (INC), visant à connaître l'exposition aux risques des internautes ainsi que son niveau de notoriété auprès du grand public, que la moitié des répondants affirme ne pas savoir à qui s'adresser en cas de problème et ne sait pas donner spontanément de nom de sites ou d'organismes pour les aider en cas de cybermalveillance. L'étude souligne, en outre, qu'en notoriété assistée, 43 % des internautes déclarent avoir

[45] Le top 5 de ces publications en nombre d'impressions a concerné exclusivement des alertes liées à la crise sanitaire (recommandations pour le télétravail en situation de crise, faux kits de confinement, etc.) ; *source RA 2020 GIP ACYMA.*

[46] Voir annexe n°6. Le Club de sécurité de l'information français parle d'« u*ne vulnérabilité des entreprises aux cyber-attaques toujours avérée »*, précisant que « *57 % des entreprises déclarent avoir connu au moins une cyber-attaque en 2020 : une vulnérabilité toujours présente donc, malgré un taux en légère baisse par rapport à l'année dernière [2020] (65 %)* » et qu'« *une entreprise sur 5 (19 %) a été victime d'une attaque de type rançongiciels provoquant un chiffrement ou un volet chantage de données.* »

entendu parler de *www.cybermalveillance. gouv.fr* et que 7 % d'entre eux ont utilisé le service. La première source de notoriété est la recherche sur Internet (31 %), suivie de la presse (15 %) puis le bouche-à-oreille (9 %).

Ce déficit de notoriété est également pointé dans un rapport d'information du Sénat de juillet 2020[47] précisant qu'un effort de prévention doit être renforcé, notamment par une plus grande sensibilisation du grand public, citant le GIP ACYMA et recommandant de *« sensibiliser l'opinion publique, et notamment les plus jeunes, aux enjeux de la cybersécurité, grâce à des campagnes d'information et en mobilisant l'éducation nationale. »*

La commission supérieure du numérique et des postes (CSNP), s'agissant de la sensibilisation et de la formation à la sécurité numérique, recommande également dans un avis aux pouvoirs publics[48] de « *développer une politique massive d'information et de sensibilisation de la population sur les risques encourus dans l'espace numérique, tant à titre privé que professionnel, et sur les mesures et dispositions permettant de s'en prémunir. »*

Le premier niveau de sécurité numérique étant individuel, ce déficit de notoriété du GIP et de la plateforme *Cybermalveillance.gouv.fr* mérite d'être comblé par une communication accrue visant un large public pour aider à mieux comprendre les risques numériques et pour donner les bons réflexes en cas d'attaque. De même, il paraît souhaitable d'étendre les partenariats plus spécifiques, tels que le GIP en a établis en 2019 et 2020 afin de développer des actions ciblées auprès des populations ou encore renforcer les échanges opérationnels avec la section J3 cybercriminalité (juridiction interrégionale spécialisée – JIRS) du parquet de Paris et les services d'enquête de police judiciaire (voir annexe n°5).

Recommandation n° 1. Renforcer la notoriété du GIP ACYMA auprès des différents publics cibles, notamment les jeunes, les TPE et les PME. (SGG, SGDSN, ANSSI, GIP)

1.2.1.3 Un observatoire de la menace à mettre en œuvre dans un contexte interministériel

L'anticipation de la menace cyber passe par l'observation du risque numérique avec un dispositif de surveillance adapté aux structures à protéger et des solutions techniques pour remédier aux impacts constatés à la suite d'une attaque, quelle que soit sa nature. Cette mission figure dans l'arrêté du 3 mars 2017 portant approbation de la convention constitutive du GIP ACYMA : « *Le Groupement a pour objet d'assurer : [...] 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. »*

Cette observation des risques numériques a été amorcée en 2018 par le GIP et formalisée en 2019 par la production d'indicateurs présentant l'état de la menace à partir de l'analyse des

[47] Rapport d'information n°613, relatif à la lutte contre la cybercriminalité (p.9 et 46) : *« Le GIP Acyma diffuse de l'information via son site* www.cybermalveillance.gouv.fr*, d'abord en direction du grand public. S'il a gagné en notoriété ces dernières années, son action pourrait être relayée par des campagnes d'information régulières dans les grands médias généralistes, sur la modèle de la campagne que le GIP a conçue en 2019 avec l'Institut national de la consommation (INC), diffusée sur France Télévision et sur des chaînes de la TNT. »*

[48] Avis n°2021-03 du 29 avril 2021 portant recommandations dans le domaine de la sécurité numérique - recommandation n°10 – p.5.

recherches d'assistance des différentes catégories de publics pour *in fine* prévenir les risques et adapter l'offre de service. Ces indicateurs ont par ailleurs été affinés en 2020 pour présenter des statistiques différenciées par types et catégories de publics (voir *supra*), plus facilement exploitables.

Le GIP a lancé au second semestre 2019 un groupe de travail interne réunissant ses membres désireux de contribuer à ce projet, pour élaborer des propositions sur le périmètre, l'organisation et les moyens nécessaires à la constitution de ce futur observatoire. Les conclusions attendues initialement fin 2020 restent pendantes. En dehors des statistiques de qualité produites par le GIP, la mise en place de cet observatoire de la menace n'est pas effective et les capacités d'exploitation « stratégique, tactique et technique » des données ne sont pas réalisées.

Ces travaux internes au GIP doivent rapidement aboutir à des propositions concrètes à présenter en conseil d'administration.

1.2.2 Un continuum du traitement des actes de cybermalveillance à renforcer

1.2.2.1 Un environnement de sécurité foisonnant

1.2.2.1.1 La cybersécurité implique toutes les forces de sécurité intérieure

Depuis le 25 février 2021, la direction générale de la gendarmerie nationale s'est dotée d'un commandement de la gendarmerie dans le cyberespace (ComCyberGend), rattaché au directeur général. Regroupant l'ensemble des 7 000 cyber-enquêteurs de la gendarmerie, il est chargé d'établir l'état de la menace cyber, d'animer, de coordonner, de mettre en cohérence, de renforcer et de rendre plus visibles les capacités de la gendarmerie dans le domaine cyber. Il intègre notamment un centre de lutte contre les criminalités numériques (C3N), chargé des investigations les plus complexes sur Internet et de l'identification des phénomènes émergents, que complètent une division d'appui aux opérations numériques (DAONUM), une division chargée du volet prévention et proximité numérique et une division en charge de la stratégie, de la prospective et des partenariats. Il coordonne également le réseau des enquêteurs technologies numériques (NTECH) et leurs correspondants (C-NTECH) répartis sur l'ensemble du territoire métropolitain et outre-mer.

La direction générale de la police nationale a créé en 2014 la sous-direction de la lutte contre la cybercriminalité (SDLC) au sein de la direction centrale de la police judiciaire (DCPJ). Pôle de compétence nationale, la sous-direction dispose notamment de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) et travaille en partenariat avec les autres administrations du ministère de l'intérieur et avec d'autres administrations centrales, telles que la direction générale de la concurrence, de la consommation et de la répression des fraudes ou la direction générale des douanes et des droits indirects.

La préfecture de police de Paris s'est dotée en 2019 d'une brigade de lutte contre la cybercriminalité (BL2C) compétente sur le ressort de Paris et de la petite couronne. Elle prenait le relai de la brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) créée

en 1994. La BL2C est en charge de la lutte contre les atteintes aux systèmes d'information (piratages de base de données, extractions de données à caractères personnels, attaques par rançongiciels, attaques en déni de service, etc.).

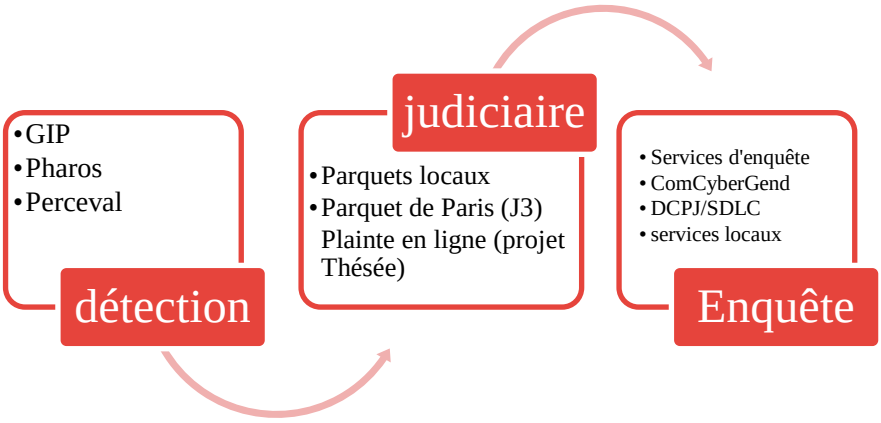
À ces organismes, s'ajoute au sein du ministère de l'intérieur, la délégation ministérielle aux partenariats, aux stratégies et aux innovations de sécurité[49] (DPSIS) qui coordonne et anime les partenariats entre tous les acteurs de la sécurité[50]. La DPSIS est organisée autour de quatre pôles consacrés aux innovations et cybermenaces, aux acteurs de la sécurité, aux professions et territoires exposés et à la normalisation.

Enfin, au travers du *Livre blanc de la sécurité intérieure* de 2020[51], s'agissant de la cybersécurité, le ministère de l'intérieur veut « *apporter une réponse globale et coordonnée face une menace croissante* ». Devant « *la nécessité d'accroître le pilotage ministériel des enjeux relatifs aux cybermenaces* », le livre blanc prévoit la création « *d'une délégation ministérielle aux partenariats, aux stratégies et aux innovations de sécurité* – voir *supra* – (…) *et d'un service central à compétence nationale* [SCN], *bi-force, placé sous la tutelle du ministre, rattaché organiquement à la direction générale de la gendarmerie nationale* ». Le livre blanc précise que cette réponse globale aux enjeux de cybersécurité impliquera de prendre en compte une série de missions, notamment « *établir l'état de la menace, élaborer et mettre en œuvre la stratégie du ministère de l'intérieur dans un cadre interministériel, coordonner les actions stratégiques et opérationnelles des différents acteurs*[52]*, au plan central et dans les territoires, dans le domaine de la prévention, de la protection, de l'innovation, de la gestion des crises et de l'action répressive, en renseignement comme en judiciaire, dans la détection et l'entrave d'attaques cybernétiques ayant une origine ou une influence étatique […]*. »

La création de ce service à compétence nationale parallèlement à la DPSIS pose la question de la répartition des missions entre eux et, au-delà de son positionnement au sein de la gendarmerie nationale, de l'autorité fonctionnelle qu'il exercera ou non sur les acteurs du ministère de l'intérieur dans le domaine de la cybersécurité, ainsi que le niveau de représentation qu'il lui sera donné dans les instances supérieures interministérielles de coordination et de pilotage de la cybersécurité. Enfin, comme évoqué *supra* le positionnement de l'observatoire de la menace cyber vis-à-vis de ce SCN mérite d'être étudié.

[49] Décret n° 2020-1126 du 11 septembre 2020. La DPSIS fusionne trois entités : la délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC), la délégation aux coopérations de sécurité (DCS) et la mission ministérielle de normalisation.
[50] Forces de sécurité intérieure, policiers municipaux, entreprises de la sécurité privée, services de sécurité internes, opérateurs de transports, bailleurs sociaux, dispositifs de participation citoyenne.
[51] Livre blanc de la sécurité intérieure –novembre 2020, Troisième livret, paragraphe 1.3.1 -pages 183 à 185.
[52] Sans préjudice du rôle exclusif de la DGSI dans ses domaines d'action.

Schéma n° 1 : Le continuum de sécurité



Source : Cour des comptes

1.2.2.1.2 Les dispositifs de signalement par le public sont aussi nombreux que peu connus

Le GIP n'est que l'un des acteurs des dispositifs de signalement offert au public. Il paraît d'ailleurs difficile pour les « victimes » de se repérer dans un univers où les acteurs de prévention, de signalement ou d'assistance souffrent à la fois d'une très faible notoriété et d'une complexité des procédures selon le type de menace.

Tableau n° 1 : Principaux dispositifs d'assistance au public en cas de cyber-agression

Nom de la plateforme	Opérateur	Objet	Type de menace	Public visé
Signal-SPAM	Association loi de 1901 regroupant acteurs publics et privés	Signalement	Courrier électronique non sollicité ou malveillant	Grand public
Plateforme d'analyse, de recoupement et d'orientation des signalements (**Pharos**)	Ministère de l'intérieur (SDLC)	Signalement	Contenu illicite sur internet	Grand public
Traitement harmonisé des enquêtes et signalement pour les e-escroqueries (**THESEE**)	Ministère de l'intérieur (SDLC)	Signalement et plainte en ligne (projet)	E-escroqueries	Tous publics
Phishing initiative	Orange Cyberdéfense	Signalement	Hameçonnage	Grand public

Info escroqueries	Ministère de l'intérieur (SDLC)	Information	Escroqueries en ligne	Grand public
33700	Association française du multimédia mobile (AFMM)	Signalement	SMS indésirables	Grand public
Perceval	Ministère de l'intérieur	Signalement	Fraude à la carte bancaire	Grand public

Source : Cour des comptes

L'association Signal SPAM est par ailleurs également membre du GIP cybermalveillance. Le foisonnement des dispositifs, qui peut s'expliquer par le caractère relativement nouveau du sujet, ne permet pas aux « victimes » de distinguer facilement l'interlocuteur auquel elles sont censées s'adresser.

Le dispositif THESEE (traitement harmonisé des enquêtes et signalement pour les e-escroqueries) a pour but de faciliter le dépôt de plainte en ligne pour les actes de cybermalveillance relevant de l'escroquerie en permettant un signalement pouvant déboucher sur une plainte via le portail service-public.fr. Le service devait ouvrir en 2020 mais n'était toujours pas opérationnel à la fin de 2021.

Il n'existe donc pas de guichet unique pour l'usager, même si les sites des différents acteurs renvoient volontiers les uns sur les autres. Le rapprochement de certains acteurs, ou au moins de leur mode de saisine pourrait contribuer à clarifier le paysage de l'assistance et du signalement des victimes. Un point d'entrée unique pourrait permettre de mieux orienter l'usager et faciliter le développement de la notoriété nécessaire au développement de ce type de service en ligne.

En réponse aux observations provisoires de la Cour, le GIP Acyma souligne que l'article 2 de sa convention dispose la mise en place d'un « guichet unique » est une mission d'intérêt général portant sur l'assistance aux particuliers, aux entreprises et aux administrations victimes d'actes de cybermalveillance. Il est donc fondamental, selon le GIP, que chaque acteur public et privé puisse respecter ce principe de guichet unique dans l'intérêt d'une politique publique efficace et un meilleur service rendu aux victimes.

1.2.2.2 La notion de victime est appréciée différemment par le GIP et les forces de police

La sous-direction de la lutte contre la cybercriminalité (SDLC) de la direction centrale de la police judiciaire (DCPJ) considère que seule peut être qualifiée de victime une personne qui a porté plainte, alors que le groupement considère que toute personne s'étant connectée sur sa plateforme et ayant signalé avoir fait l'objet d'un acte de cybermalveillance est une victime.

La SDLC déplore le faible nombre de plaintes émanant du grand public et considère qu'une plainte en escroquerie au niveau local a peu de chance de prospérer du fait du seuil d'intervention du parquet, des faibles moyens d'enquêter localement. La plainte de la victime

débouche le plus souvent sur une simple main courante. La mise en œuvre du dispositif THESEE (voir *supra*), sans filtre des services de police de proximité, pourrait donc être plus propice à développer ce type de plainte, pour peu qu'il soit suffisamment connu des victimes potentielles.

L'une des difficultés rencontrées dans les affaires de cybermalveillance, selon les enquêteurs, est la destruction de preuves numériques. En effet, les prestataires ou les victimes elles-mêmes, effacent parfois les supports numériques infectés pour réinstaller les systèmes sans toujours conserver les traces permettant l'identification et la poursuite des malfaiteurs. Le GIP assure inciter les prestataires qu'il référence à privilégier autant que possible la conservation des preuves pour les services d'enquête et n'a pas été, à ce jour, informé d'un quelconque manquement caractérisé, hors les cas où la victime demande à son prestataire de rétablir son système sans délai en faisant fi des preuves.

1.2.2.3 Le rôle du parquet et celui du ministère de la justice doivent s'affirmer

L'action pénale des parquets est rendue complexe par le caractère souvent national ou transnational des affaires et par l'insuffisance des compétences locales sur une criminalité à caractère technique souvent très spécialisée. L'agrégation du nombre des victimes au plan national peut parfois conduire, en outre, à obtenir un total significatif là où une affaire individuelle est parfois peu susceptible d'aboutir même si une plainte est déposée.

Les moyens dévolus à ce contentieux par la Chancellerie apparaissent faibles. La direction de l'action pénale par le ministre de la justice n'est assurée que par un simple chargé de mission auprès du directeur des affaires criminelles et des grâces[53]. Ce dernier assure non seulement la cohérence de l'action pénale des parquets au moyen de dépêches thématiques mais également la liaison avec le ministère de l'intérieur, la représentation du ministère dans les instances interministérielles (centre de coordination des crises cyber – C4 – piloté par le SGDSN) et au sein des différents organes de coordination de l'Union européenne (Eurojust notamment).

Par ailleurs, une compétence nationale concurrente est conférée à la section J3 du Parquet du tribunal judiciaire de Paris pour les affaires de cybercriminalité complexes (pluralité de victimes ou d'auteurs sur le territoire national, dimension internationale forte, technicité ou complexité du mode opératoire, qualité de la victime[54]). Le rapport des sénateurs Sophie Joissains et Jacques Bigot sur la lutte contre la cybercriminalité[55] notait en juillet 2020 que *« les moyens du parquet spécialisé […] mériteraient d'être considérablement augmentés »* jugeant qu'*« un effectif de trois magistrats pour traiter les affaires de dimension nationale et internationale et animer un réseau de référents est notoirement insuffisant »*. Cet état de fait implique, comme le soulignaient les sénateurs, que *« la section J3 adapte le nombre de ses saisines à sa capacité à les traiter. Elle renonce régulièrement à se saisir de dossiers dont la complexité pourrait pourtant justifier une centralisation parisienne »*.

[53] Mission de prévention et de lutte contre la cybercriminalité.
[54] OIV ou administration centrale, par exemple.
[55] Rapport n° 613 fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) et de la commission des affaires européennes (2) sur la lutte contre la cybercriminalité, juillet 2020.

De même, la commission supérieure du numérique et des postes (CNSP) notait également dans son avis du 29 avril 2021 le décalage entre les moyens humains du Parquet et l'augmentation du *« nombre d'attaques […] à un rythme exponentiel depuis deux ans »*, préconisant l'étude par le Gouvernement de la *« création d'un parquet national cyber, disposant des ressources et des expertises suffisantes pour instruire les dossiers liés aux affaires de cyber-délinquance les plus complexes »*.

En dehors de la spécialisation de l'OCLCTIC, s'agissant des affaires confiées à la police nationale, sur les affaires de rançongiciels et de sa co-saisine systématique comme chef de file, l'attribution des enquêtes semble plus dépendre, selon les services interrogés, d'une logique capacitaire et de la disponibilité des services compétents que de réelles spécialisations techniques. Le ComCyberGend et la BL2C de la préfecture de police de Paris se voient eux aussi confier des affaires relatives aux familles de rançongiciels dont ils ont la charge.

Malgré une bonne prise en compte du fait cyber, les équipes en charge des affaires de cybercriminalité sont par ailleurs sous-dimensionnées pour traiter un volume d'affaires croissant.

Au-delà du renforcement des capacités d'investigation et de traitement judiciaires des affaires, il convient de densifier les liens existants entre tous les acteurs étatiques du « continuum cybermalveillance » pour une toujours plus grande coordination et synchronisation de la lutte contre la cybercriminalité. Cela implique nécessairement un travail conjoint du ministère de l'intérieur avec le ministère de la justice, intégrant le GIP ACYMA comme un contributeur majeur à ce continuum.

Recommandation n° 2. Densifier les liens entre tous les acteurs étatiques du « continuum cybermalveillance ». (Ministère de l'intérieur, ministère de la justice, GIP)

1.3 La gouvernance : un lien fort à conserver avec l'État

Dès sa création, le GIP a entretenu une relation forte avec l'État puisqu'il a été conçu pendant près d'un an au sein de l'ANSSI avant de disposer de ses propres locaux et de son propre personnel. La gouvernance d'ACYMA est constituée par un conseil d'administration et une assemblée générale réunissant les membres afin de statuer sur le fonctionnement et la stratégie du dispositif.

1.3.1 Le GIP est un organisme associant le public au privé mais qui repose principalement sur la puissance publique

Le groupement organise ses membres en quatre collèges qui élisent leurs représentants au conseil d'administration en assemblée générale[56] :

- le premier est composé des représentants de l'État, notamment le Premier ministre, le ministre de l'intérieur, le ministre de la justice, le ministre de l'économie et des finances, le secrétaire d'État chargé du numérique, la ministre des armées ;
- le deuxième est composé des représentants des utilisateurs ou des usagers ;
- le troisième est composé des représentants des prestataires de services ;
- le quatrième collège est composé des représentants des offreurs de solutions et de services ou directement des offreurs de solutions et de services.

L'État dispose d'autant de représentants que de ministères figurant dans le collège, mais possède en revanche statutairement 52 voix sur 100, comme le précise le tableau n°2.

Tableau n° 2 : Répartition des représentants et des droits de vote

Collèges	Nombre de voix	Nombre de représentants
État	52	6 titulaires et 6 suppléants (Au 31/12/2021)
Collège utilisateurs	16	2 titulaires et 2 suppléants
Collège prestataires	16	2 titulaires et 2 suppléants
Collège offreurs	16	2 titulaires et 2 suppléants

Source : statuts du GIP Acyma

Les trois autres collèges peuvent regrouper des organisations très diverses. Ainsi, le collège « utilisateurs » comprend principalement des associations de consommateurs, mais aussi des collectivités ou leur représentant (Région Pays de Loire, l'association Régions de France, Avicca, Coter Numérique et Déclic). Le collège « prestataires » comprend le syndicat professionnel Numeum (anciennement Syntec numérique) alors que le MEDEF figure au sein du collège utilisateurs.

Le président du groupement est actuellement le directeur général de l'ANSSI.

[56] Arrêté du 13 novembre 2020 portant approbation des modifications de la convention constitutive du groupement d'intérêt public dénommé « Groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance ».

1.3.2 Une participation plus importante du secteur privé, pourtant souhaitable, semble difficilement envisageable à court terme

Par son financement (voir *infra*), le groupement associe certes le public) au privé mais la part de la puissance publique reste largement prépondérante (environ 60 % des ressources financières en 2021) même si la part du financement privé est en hausse constante depuis 2018.

Les contributions annuelles des membres issus du secteur privé apparaissent faibles au regard de leurs ressources (voir *infra*) et la fidélisation des plus petits acteurs reste difficile à établir. Le retour sur investissement de leurs contributions est faible, car chaque membre a droit au même mode d'affichage sur le site ou dans la documentation du groupement quel que soit le montant de sa contribution.

Le mécénat d'entreprise ou le parrainage permettent de mettre en avant un partenaire en fonction de sa contribution. C'est pourquoi le groupement envisage de recourir à d'autres formes de financement, telle que l'appel public à la générosité ou le mécénat, qui offrent en outre un avantage fiscal non négligeable aux donateurs (voir *infra*).

En réponse aux observations provisoires de la Cour, le groupement indique qu'il a veillé à éviter les conflits d'intérêts, notamment avec les prestataires référencés sur sa plateforme de mise en relation avec les victimes d'actes de cybermalveillance, par la signature d'une charte d'engagement lors de la demande de référencement qui est étudiée individuellement. Une charte d'éthique signée par l'ensemble des membres complète le dispositif.

CONCLUSION INTERMÉDIAIRE

L'action du GIP ACYMA complète la stratégie de cybersécurité française pour des populations à la fois nombreuses, diffuses et vulnérables, pour lesquelles l'ANSSI n'apportait pas, en 2015, de réponse adaptée.

Le caractère transnational de la menace, avec des victimes et des criminels appartenant à des ensembles nationaux ou régionaux parfois radicalement différents a entraîné une réponse forte en matière de coopération internationale, en particulier s'agissant des instruments juridiques. Le paysage des acteurs nationaux, notamment des forces de sécurité chargées de lutter contre la cybercriminalité, apparaît en revanche beaucoup plus fragmenté.

Le foisonnement de services d'enquête et de plateformes de signalement est en outre difficilement lisible pour le citoyen et nécessite probablement une coordination coûteuse en énergie et en temps. Les moyens modestes de l'action judiciaire contrastent avec la croissance de la menace.

La création d'un organisme associant puissance publique, organismes publics, collectivités et acteurs privés, chargé de prévenir les cybermenaces, de sélectionner les prestataires aidant les victimes et de les mettre en relation et enfin d'observer l'évolution de la menace cyber ne connaît pas d'équivalent, au plan européen au moins. Si les missions de prévention et d'assistance dévolues au GIP ACYMA ont pris un véritable essor, la mission d'observation reste à préciser en termes d'objectifs et de positionnement du GIP dans la mesure où nombre d'acteurs de niveau ministériel ou interministériel en sont également contributeurs et responsables.

Le groupement reste largement dépendant de la puissance publique, dans sa gouvernance comme dans son financement, alors même que la perspective d'associer le secteur privé, outre les aspects d'engagement et de responsabilisation des membres, avait pour but de fournir des ressources financières substantielles permettant de financer la mission d'intérêt général dans un contexte budgétaire contraint.

---

2 DES MOYENS SUFFISANTS POUR LE LANCEMENT DU GIP, MAIS QUI DEMANDENT À ÊTRE RENFORCÉS.

Avec un premier niveau opérationnel atteint en 2020, le GIP affiche une gestion équilibrée des ressources dont il dispose, parfois au détriment de la réalisation de certains objectifs. Reposant largement sur un financement public, les ressources financières du groupement doivent poursuivre leur diversification et, surtout, être mises en adéquation avec les missions et les objectifs qui lui ont été confiés par ses membres et par ses tutelles. Ce renforcement budgétaire devra s'accompagner d'un soutien administratif plus conséquent et s'inscrire dans le cadre d'un suivi plus précis du budget.

2.1 Une situation financière équilibrée

Le groupement présente une situation financière équilibrée avec des fonds propres et une trésorerie stable. L'exécution budgétaire a atteint un palier qui n'est pas à la hauteur des ambitions initiales, faute de ressources suffisantes.

2.1.1 Des fonds propres et une trésorerie stable

Personne morale de droit public, le GIP ACYMA est un organisme national à caractère administratif ayant pour objet une mission d'intérêt général. Le groupement est constitué sans capital, et administré par un conseil d'administration présidé par le directeur général de l'ANSSI, et par une assemblée générale composée des membres du groupement réunis en quatre collèges.

Les fonds propres sur la période 2017-2020 sont stables à compter de l'année 2018, l'exercice comptable 2017 n'ayant duré que deux mois. Le financement de l'actif par l'État correspond au budget primitif du GIP financé par le SGDSN qui prévoyait un volet investissement en complément des dépenses de fonctionnement[57].

---

[57]Le comptable a indiqué que les dispositions du BOFIP-GCP 13-004 du 31 janvier 2013, qui prévoit les modalités de comptabilisation des financements externes de l'actif applicable aux EPN et GIP, avaient été appliquées mais

Tableau n° 3 : Évolution des fonds propres sur la période 2017-2020 (en euros)

	2017	2018	2019	2020
Financement de l'actif par l'État	14 793	11 982	9 171	9 171
Report à nouveau	-	258 499	598 637	587 345
Résultat	258 499	340 138	<11 292>	11 085
Fonds propres	**273 292**	**610 619**	**596 516**	**607 601**

Source : Cour des comptes, d'après les comptes annuels du GIP ACYMA

La trésorerie du GIP est relativement stable sur la période et fait l'objet d'un suivi en lien avec l'exécution budgétaire.

Tableau n° 4 : Trésorerie 2017-2020 (en euros)

	2017	2018	2019	2020
Disponibilités	272 185	523 890	448 591	496 717

Source : Cour des comptes, d'après les comptes annuels du GIP ACYMA

2.1.2 L'exécution budgétaire a atteint un palier

Le rapport de présentation du compte financier 2020 mentionne que l'exécution budgétaire transcrite dans ce compte retrace « *un équilibre de gestion en recettes et en dépenses très satisfaisant* ». Malgré un contexte difficile en 2020 du fait de la crise sanitaire, notamment au regard de ses actions de communication, le GIP a maintenu l'essentiel de ses actions sans dérapage financier. L'évolution des résultats (cf. tableau n°3) atteste de la recherche d'un résultat à l'équilibre (+ 11 292 € en 2019 et – 11 084 € en 2020) tel que l'implique le fonctionnement d'un GIP. Si les résultats précédents ont permis de constituer une réserve financière pour le GIP ACYMA, celle-ci a été intégralement consommée en 2020 avec la livraison de la plateforme informatique affectée à la mission du GIP.

Le comptable précise que le fonds de roulement demeure dans la norme et permet un fonctionnement normal et sécurisé mais ne pourra être sollicité pour les projets à venir. Il souligne également que le volume budgétaire moyen retenu lors de la création du GIP (2,5 M€ annuel) n'est pas atteint et qu'il conviendrait dès 2021 de budgéter les dépenses d'investissement en préservant l'équilibre actuel du fonds de roulement (comme cela a été

que le financement proposé ne distinguait pas les dépenses de fonctionnement de celles d'investissement, la somme étant librement exécutée au moyens des budgets votés par l'assemblée délibérante. Cette ligne aurait dû être consommée dans l'exercice suivant afin de solder ce financement de l'actif par l'État qui n'est qu'initial mais perdure au fil des exercices, faute d'être consommé. Le comptable s'est engagé à liquider ce financement par l'État dans les meilleurs délais.

demandé par l'assemblée délibérante lors des précédents exercices). Le niveau des dépenses actuelles est compatible avec les ressources, mais faute de nouveaux financements, les recrutements et les investissements resteront limités.

Tableau n° 5 : Évolution des résultats du GIP ACYMA 2017-2020 (en euros)

	2017	2018	2019	2020
Produits de fonctionnement	326 906,51	1 169 299,19	1 195 122,25	1 399 797,52
Charges de fonctionnement	68 407,67	829 160,67	1 206 414,94	1 388 712,65
Résultat de fonctionnement (I)	258 498,84	340 138,52	- 11 292,69	11 084,87
Produits financiers	-	-	-	-
Charges financières	-	-	-	0,02
Résultat financier (II)	-	-	-	– 0,02
Résultat (I+II)	258 498,84	340 138,52	– 11 292,69	11 084,85

Source : Cour des comptes, d'après les comptes annuels du GIP ACYMA

2.2 Des produits à diversifier

Les produits de fonctionnement du GIP ACYMA sont en constante progression sur la période 2017-2021 et proviennent à la fois de source publique (principalement par la subvention accordée par l'ANSSI via le SGDSN) et privée (contributions des sociétés membres). Les sources de financement initialement majoritairement publiques sont réparties autour de 45 % de subventions de l'État, 5 % de subventions provenant d'autres entités publiques (La Poste et la caisse des dépôts et consignations) et 50 % de contributions privées en 2020. Cette tendance se confirme en 2021, exception faite de la subvention publique exceptionnelle accordée dans le cadre du plan France relance.

Tableau n° 6 : Les principaux produits de fonctionnement du GIP ACYMA 2017-2020 (en euros)

	2017	2018	2019	2020	Prévisions 2021
Subventions de l'État	326 800	736 488	636 510	633 500	630 606 + 691 000[58]
Subventions autres entités publiques[59]	0	25 000	25 000	61 000	0
Dons, legs, mécénat	0	0	15 000	0	0
Contributions financières des membres	0	405 000	515 000	705 000	886 000
Produits de fonctionnement	**326 800**	**1 166 488**	**1 191 510**	**1 399 500**	**2 207 806**

Source : Cour des comptes, d'après les comptes annuels du GIP ACYMA.
Les quatre emplois mis à disposition par des administrations en 2020 (voir infra*) pourraient être considérés comme des subventions publiques. Leur coût total est estimé par la Cour à 300 000 euros en première approche.*

2.2.1 La subvention versée par l'ANSSI constitue la principale ressource financière du groupement

Le poids de la subvention accordée au GIP ACYMA par l'ANSSI (via le SGDSN) est de l'ordre de 54 % sur la période 2018-2020. Pendant la phase d'incubation (en 2017), le GIP avait bénéficié principalement d'une subvention accordée par l'ANSSI de 326 800 € ainsi que de mobiliers, prestations de système d'information et de prestations évènementielles prises en charge par le SGDSN.

Le premier budget de plein exercice de l'établissement est retracé dans le compte financier 2018. Le rapport de présentation du compte financier 2018 mentionne que le précédent exercice comptable ne transcrivait qu'un dixième de l'activité du GIP et ne renseignait que très partiellement les données patrimoniales et financières du GIP ; la tutelle financière et logistique de l'ANSSI s'étant exercée jusqu'au mois de novembre 2017.

Les éléments fournis par le GIP précisent que les frais engagés par le SGDSN lors de la phase d'incubation ont été de 560 937 € en CP. Ces frais regroupent des dépenses de loyers, de frais d'agence, de travaux, de personnels, de fournitures de bureau (Lyreco), de logiciels, d'imprimantes, écrans et projecteurs. L'ANSSI a pendant la période d'incubation du GIP pris

[58] Il s'agit d'une subvention exceptionnelle versée au titre de l'année 2021 dans le cadre du plan France relance dont le SGDSN, et en son sein l'ANSSI, est attributaire de crédits avec pour objectif d'accélérer la sécurisation des systèmes numériques de l'État et des territoires face aux risques numériques.
[59] Les subventions de La poste et de la caisse des dépôts ont été portées en « autres subventions publiques » soit 25 000 € pour 2018-2019 et 2020 pour La poste et 36 000 € pour la caisse des dépôts au titre de l'année 2020.

en charge sur son budget du matériel de bureau et le paiement de loyers sans que cela n'apparaisse dans l'inventaire ni ailleurs.

Autre particularité, le loyer annuel du GIP ACYMA est pris en charge par le SGDSN depuis 2018. La subvention accordée par l'ANSSI et versée par le SGDSN est ainsi diminuée en recette à concurrence du montant de cette prise en charge. Le bail des locaux du GIP, dont le SGDSN est titulaire, mentionne à l'article 27 que le loyer des bureaux annuel hors taxes est de 110 250 € plus 1 440 € pour le parking, assorti d'une provision annuelle de charges pour le premier exercice de 24 570 € HT. La signature du bail le 3 juillet 2017[60], alors que le GIP ACYMA créé le 3 mars 2017 n'avait pas encore perçu de subvention, a été sécurisée par une convention de mise à disposition par le SGDSN datée du 3 juillet 2017. Cette convention[61] mentionne que le SGDSN met à disposition du GIP ACYMA, à titre provisoire, à compter du 1er juillet 2017, les locaux situés dans l'immeuble 6, rue Bouchardon à Paris 10e, comme composante de la contribution financière au GIP de l'Agence nationale de la sécurité des systèmes d'information, service à compétence nationale rattachée au SGDSN[62]. L'article 7 de la convention précise également que *« la présente convention de mise à disposition prendra fin à la date d'entrée en vigueur de l'avenant au contrat de bail liant le SGDSN à la MGEFI, propriétaire des locaux, et devant transférer le bénéfice du bail au GIP ACYMA. »*

Mention est faite dans les procès-verbaux de délibération adoptée par le conseil d'administration du GIP de la subvention octroyée annuellement par l'ANSSI après déduction du loyer pris en charge par le SGDSN, mais sans indication du montant des loyers déduits. Il est indiqué dans le procès-verbal de la délibération adoptée par le conseil d'administration du 13 juillet 2018 concernant l'approbation du budget prévisionnel 2019 : « *le loyer annuel du GIP étant toujours pris en charge par le SGDSN, titulaire du bail, celui-ci est déduit du montant total de la subvention de l'ANSSI (versée formellement par le SGDSN)* ». Cette subvention pour 2019 est d'un montant total de 800 000 €.[63] Le SGDSN a fourni l'arrêté du Premier ministre du 25 mars 2021 octroyant la subvention versée au GIP ACYMA ainsi que le calendrier de versement pour 2021 (250 000 € à la notification de la subvention, 250 000 € en mai et 130 206 € en septembre). Un tableau récapitulatif de l'historique des versements versés a également été fourni faisant apparaître les loyers déduits.

[60] L'article 25 du bail indique la date d'effet du bai l au 1er juillet 2017 et la date de fin de bail au 30 juin 2026 avec une durée du bail de 3 ans fermes renouvelables en deux périodes consécutives de 3 années.
[61] L'article 5 : clause financière de la convention précise que l'occupation se fera à titre gratuit, sans indemnité dans la mesure où celle-ci s'analyse comme une composante de la contribution financière de l'ANSSI.
[62] L'ANSSI, créée par décret n° 2009-834 du 7 juillet 2009, est un service à compétence nationale qui dispose sur les crédits du SGDSN des moyens nécessaires à l'accomplissement de sa mission.
[63] Dans cette même délibération de juillet 2018, le directeur général rappelle qu'il a été convenu avec l'ANSSI un financement de 900 000 € les deux premières années et de 800 000 € les années suivantes, charge au GIP de trouver d'autres financements notamment d'entités privées ou des membres étatiques.

Tableau n° 7 : Historique des versements de la subvention versée par l'ANSSI (hors plan de relance)

	Subvention sollicitée	Montant des locaux (loyers bureaux, parking, charges)	Subvention versée
2018	900 000 €	-	900 000 €
2019	800 000 €	163 490 €	636 510 €
2020	800 000 €	166 500 €	633 500 €
2021	800 000 €	169 794 €	630 206 €

Source : Cour des comptes à partir des données fournies par le SDGSN

2.2.2 Les contributions financières des sociétés membres sont significatives pour le GIP

L'article 9 de la convention constitutive du GIP ACYMA mentionne que les ressources du groupement peuvent comprendre les contributions financières des membres ; la mise à disposition sans contrepartie financière de personnels, de locaux ou d'équipements, des subventions ; des produits de biens propres ou mis à leur disposition, la rémunération des prestations et les produits de la propriété intellectuelle ; des emprunts et autres ressources d'origine contractuelle ; des dons y compris sous forme de mécénat et legs ; tout autre forme de contribution au fonctionnement du groupement.

Le montant des contributions financières des membres, hors dons et subventions des membres du collège des représentants de l'État, est déterminé dans les conditions fixées par le règlement intérieur soit quatre niveaux de contributions de respectivement 50 000 € ; 100 000 € ; 250 000 € et 500 000 €. L'article 9 du règlement intérieur mentionne que *« le niveau minimum de contribution financière de chaque membre est fixé à 50 000 €. Dans le respect d'un montant minimum de 50 000 €, les membres déterminent librement le montant de leur contribution »*. Les autres montants de 100 000 €, 250 000 € et 500 000 € sont indicatifs. Ce même article précise qu'à titre exceptionnel dans le cadre d'une nouvelle adhésion, le montant de la contribution financière peut être fixée à un niveau inférieur à 50 000 € en considération de la capacité contributive du membre, par décision du président après avis du conseil d'administration.

Le montant moyen des contributions financières des sociétés membres était de 33 571 € par membre en 2020 tel que détaillé dans le tableau n°8. Afin de s'adapter à cette réalité, le GIP ACYMA a modifié en juillet 2020 l'article 9 de la convention constitutive et le règlement intérieur en réévaluant à la hausse le montant des contributions pour les nouveaux arrivants et en maintenant le montant des contributions des entités déjà membres qui s'acquittaient d'une contribution de 25 000 €.

Les contributions doivent être versées au GIP ACYMA lors du premier trimestre de l'exercice budgétaire et au plus tard le 31 mars, sauf cas particulier justifié et accepté par le président du conseil d'administration.

Tableau n° 8 : Les contributions financières des sociétés membres en 2017-2020 (en euros)

Les sociétés membres	2018	2019	2020
ATTITUDE PREVENTION/FFA	30 000	30 000	30 000
BITDEFENDER	25 000	25 000	25 000
BOUYGUES TELECOM	25 000	25 000	25 000
ESET	25 000	25 000	25 000
HUB ONE	25 000	25 000	25 000
KASPERSKY	50 000	50 000	50 000
MICROSOFT	25 000	25 000	25 000
MMA	25 000	25 000	25 000
ORANGE CYBERDEFENSE	100 000	100 000	100 000
SFR Business Team	25 000	25 000	25 000
CROWDSTRIKE	-	25 000	25 000
HP France	-	25 000	25 000
MAIF	-	25 000	25 000
PALO ALTO NETWORKS	-	25 000	25 000
PUBLICIS	-	10 000	
ATEMPO-WOOXO	25 000	25 000	25 000
STORMSHIELD	25 000	25 000	25 000
AFNIC	-	-	25 000
GOOGLE	-	-	100 000
NEUFLIZE OBC	-	-	25 000
HARMONIE TECHNOLOGIE	-	-	25 000
CCR	-	-	25 000
Total des contributions financières	**405 000**	**515 000**	**705 000**
Contribution moyenne par membre par année	**33 750**	**30 294**	**33 571**

Source : Cour des comptes d'après les données du GIP ACYMA

Cette difficulté à diversifier les sources de financement du GIP constitue un frein pour son développement futur. Dans le cadre du plan France relance, le GIP bénéficie au titre de 2021 d'une subvention exceptionnelle de 691 000 € versée par l'ANSSI (via le SGDSN) et encadrée par une convention d'objectifs signée en 2021 entre le SGDSN et le GIP ACYMA, qui vise à :

- développer l'information et l'accompagnement à la sécurisation des systèmes d'information des bénéficiaires montant prévu dans la convention 218 000 €) ;
- développer la coopération avec les CSIRT[64] régionaux (montant prévu de 120 000 €) ;

[64] Les CSIRT, acronyme de *« Computer Security Incident Response Team »* ou CERT *(Centres for Emergency Response Team)* sont des centres d'alerte et de réaction rapide aux attaques cyber dont la finalité est de développer en région tout un système d'alerte avec le GIP ACYMA porté par les régions, en vue de responsabiliser l'ensemble des acteurs ; la politique de cybersécurité ne devant plus reposer exclusivement sur l'ANSSI.

- faire évoluer le GIP pour répondre à ses nouvelles missions de prévention et d'accompagnement cyber auprès des bénéficiaires (montant prévu de 353 000 €).

Le comptable a précisé dans son rapport de présentation des comptes de l'année 2020 que la montée en puissance de l'activité du GIP nécessitait d'une part de conforter la mission support notamment en instaurant des contrôles qualité par le contrôle interne et le contrôle hiérarchisé de la dépense[65] et, d'autre part, de renforcer à terme les effectifs car la mission support est concentrée sur une seule collaboratrice, l'assistante financière et administrative. Cette mission comprend en outre la logistique et la gestion du personnel, alors que la préparation de l'exécution financière nécessite une grande réactivité et un suivi qualité qui ne pourront être assumés par une seule personne avec la montée en puissance des missions « cœur de métier ».

Le GIP est donc à une étape charnière de son développement tant du point de vue de ses ressources de financement, du développement de ses missions et de la croissance de ses effectifs. Le développement du GIP cybermalveillance ne peut continuer à s'effectuer sans un soutien administratif plus conséquent, notamment pour ce qui concerne les achats, la gestion des ressources humaines et en particulier des recrutements et sa gestion financière. La présence d'un comptable public à mi-temps en adjonction de service paraît notoirement insuffisante pour assurer la bonne gestion d'un organisme appelé à se développer sensiblement dans les prochaines années.

En réponse aux observations provisoires de la Cour, le SGDSN estime que, dans la perspective d'une augmentation du budget, le renforcement de la gestion administrative du GIP *« pourrait s'inscrire dans le cadre d'un suivi plus précis du budget avec une restitution consolidée de l'usage des contributions des membres et des subventions publiques, auprès du conseil d'administration d'une part et des membres individuellement d'autre part. »* Le SGDSN précise en outre que *« ce pilotage devra s'appuyer sur des indicateurs précis relatifs aux objectifs fixés au GIP en assemblée générale, en application d'un plan stratégique à cinq ans* [cf. partie 3.1]. *»*

Recommandation n° 3. Renforcer la gestion administrative de la structure de direction du groupement. (GIP)

2.3 Des charges maîtrisées mais contraintes

Les deux postes les plus importants parmi les dépenses de fonctionnement sont les charges externes (51 % en 2019 et 45 % en 2020 des charges de fonctionnement) et les dépenses liées à la gestion de la masse salariale (43 % en 2019 et 45 % en 2020 des charges de fonctionnement).

[65] Le contrôle exhaustif de la dépense n'est aujourd'hui possible qu'en raison du faible flux d'opérations aux montants peu élevés.

2.3.1 La masse salariale, première dépense interne du groupement

L'évolution de la masse salariale est directement liée aux recrutements effectués par le GIP ACYMA pour remplir ses missions. L'augmentation de la masse salariale entre 2019 et 2020 alors que l'effectif des contractuels ne varie pas s'explique par l'arrivée de trois agents sur l'année 2019 (en mars, septembre et décembre)[66] dont le coût salarial est complet sur l'année 2020.

Tableau n° 9 : Évolution de la masse salariale du GIP ACYMA de 2017 à 2020 (en euros)

	2017	2018	2019	2020
Salaires et traitements	25 780,80	286 738,39	391 580,14	472 634,04
Charges sociales	7 666,58	94 371,37	131 641,36	159 785,86
Total	33 447,38	381 109,76	523 221,50	632 419,90

Source : Cour des comptes d'après les comptes annuels du GIP ACYMA

Les effectifs du GIP Cybermalveillance se composent de contractuels et d'un personnel mis à disposition, comme le précise le tableau ci-dessous.

Tableau n° 10 : Évolution des effectifs (en ETP)

Effectifs	Contractuels	Mise à disposition	Total
2017	4	1	5
2018	6	1	7
2019	8	1	9
2020	8	4	12

Source : GIP Acyma

Le GIP ACYMA bénéfice en 2020 de quatre personnes mises à disposition à titre gratuit[67], sur un effectif de 12 salariés, soit 30 % de l'effectif total. Ces mises à disposition sont encadrées par des conventions signées respectivement avec le ministère de l'intérieur et le SGDSN. Une convention de mise à disposition a été signée en 2017 et quatre en 2020. La convention de 2017 est une convention temporaire d'affectation du 31 août 2017 entre le ministère de l'intérieur, représenté par le directeur des personnels militaires de la gendarmerie nationale, et le GIP pour la mise à disposition à titre gratuit d'un officier de gendarmerie exerçant les fonctions d'officier de liaison au sein du GIP en charge de la sensibilisation et du

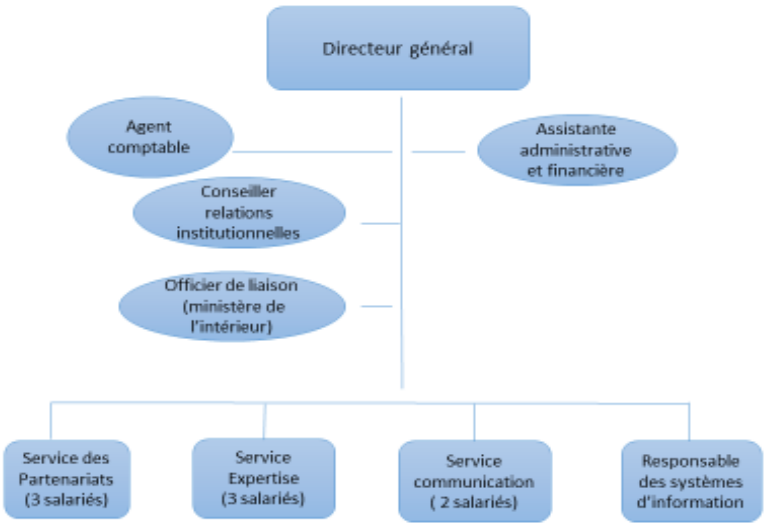
[66] Les trois nouveaux arrivants sont liés à deux créations de postes (une chargée de communication et une chargée de partenariat) et au remplacement d'un agent.
[67] L'article 42 de la loi du 11 janvier 1984 pose comme règle le remboursement des mises à disposition d'agents de la fonction publique de l'État, mais permet d'y déroger pour certains organismes publics, dont les GIP.

risque cyber. La convention prend effet au 1er mai 2017 jusqu'au 30 avril 2020 et a été prolongée par un avenant jusqu'au 31 juillet 2021.

Les trois autres mises à disposition signées en 2020 sont respectivement :

- une convention de mise à disposition gratuite à titre gracieux entre le ministère de l'intérieur et le GIP ACYMA d'une attachée d'administration d'État exerçant la fonction de conseillère. La convention prend effet le 1er septembre 2020 pour une durée de trois ans, avec possibilité de reconduction limitée à six ans ;
- une convention de mise à disposition à titre gratuit entre le ministère de l'intérieur et le GIP ACYMA d'un commandant de police fait le 15 juillet 2020 ;
- une convention de mise à disposition à titre gratuit entre le SGDSN et le GIP ACYMA d'un agent de 1re catégorie du SGDSN à compter du 14 septembre 2020 pour une durée de trois ans renouvelable.

Organigramme n° 1 : Organigramme du GIP Cybermalveillance



Source : Cour des comptes à partir des données du GIP Acyma

Le GIP a précisé que les contributions des membres mettant à disposition des agents ne sont pas actuellement valorisées dans les comptes car il ne dispose pas des fiches financières de chacun des agents mis à disposition. À ce jour, le GIP ne dispose pas des éléments leur permettant d'intégrer ces données financières dans les comptes financiers (compte de classe 8).

Cette mise à jour doit être réalisée dans le prochain compte financier de l'année 2021[68], après obtention des fiches financières, afin d'appréhender le coût réel de la masse salariale qui reste minoré dans les documents budgétaires et financiers.

[68] Les documents budgétaires de l'année 2021 pourront également faire ressortir le coût partiel des soutiens accordés à titre gratuit par le SGDSN lors de la préfiguration du GIP Acyma, non comptabilisés jusqu'à présent.

Recommandation n° 4. Intégrer la valorisation du personnel mis à disposition dans les comptes financiers afin d'évaluer le coût réel de la masse salariale du GIP ACYMA. (GIP)

2.3.2 Les dépenses de communication constituent depuis 2018 le premier poste des charges externes

Les dépenses les plus importantes parmi les charges externes concernent les prestations extérieures informatiques et les dépenses de communications (frais de publicité, publications, relations publiques). Elles ont permis de répondre aux missions d'assistance aux particuliers, aux entreprises et aux collectivités territoriales victimes d'acte de cybermalveillance avec la mise en service de la plateforme du GIP, et de mener des opérations de sensibilisation auprès des différents publics (particuliers, entreprises, collectivités locales) pour qualifier, détecter et éviter les actes de cybermalveillance.

Le budget communication en 2020 a également permis d'engager une prestation de conseils juridiques pour accompagner le GIP dans ses missions notamment pour la commande publique et la recherche de nouvelles sources de financement comme la demande de rescrit du 11 mai 2020 déposée auprès de l'administration fiscale pour développer le mécénat.

Tableau n° 11 : Évolution des charges externes de 2017 à 2020 (en euros)

Charges externes et autres achats	2017	2018	2019	2020
Locations mobilières	1 896	903	1 313	319
Études et recherche	-	-	21 000	17 736
Honoraires	-	12 600	35 120	42 078
Frais de colloques, séminaires, conférences	-	3 946	10 846	-
Foires et expositions	10 200	69 900	94 032	26 808
Publicité, publications, relations publiques	-	139 545	212 598	159 205
Catalogues et imprimés	-	8 025	14 951	29 166
Voyages et déplacements	-	5 042	5 513	1 458
Missions	159	1 493	2 941	2 154
Réceptions	521	5 956	5 283	2 626
Frais postaux et télécommunications	775	13 460	11 611	17 077
Prestations extérieures informatiques	21 392	120 843	89 290	245 210
Autres prestations extérieures diverses	-	-	67 320	15 024
Total autres achats et charges externes	**42 356**	**404 878**	**620 584**	**625 541**

Source : Cour des comptes d'après les comptes annuels du GIP ACYMA

Les dépenses de communication représentent une part non négligeable des charges externes (de l'ordre de 34 % en 2019 et 25 % en 2020). Le pôle communication du GIP ACYMA est concentré sur trois missions principales : d'une part le développement de la notoriété pour faire connaître aux publics cibles le dispositif de la plateforme cybermalveillance ; d'autre part la sensibilisation à la cybermenace en adaptant les messages auprès du grand public pour prévenir la cybermalveillance et, enfin, la communication auprès des membres du GIP pour qu'ils agissent sur leur propre public (exemple d'une campagne de sensibilisation auprès des élus locaux par le biais d'une vidéo mettant en situation une attaque dans une collectivité locale).

Afin de mieux relayer l'information, le GIP développe la fréquentation de son site internet par l'amélioration du référencement sur les moteurs de recherche, la présence sur les réseaux sociaux comme twitter qui nécessite peu de budget et par le biais d'une lettre d'information. Il organise des évènements comme celui de la fin juillet 2019, consistant en une distribution de dépliants aux voyageurs à la gare de Lyon au moment des départs en vacances décrivant les actes de cybermalveillance et les réflexes à développer. Il participe également à des salons dont un au côté de l'ANSSI[69].

La principale difficulté rencontrée par le pôle communication réside dans l'absence de moyens budgétaires pour toucher un large public par le biais de grandes campagnes de sensibilisation d'ampleur, estimées à quatre millions d'euros par an selon le GIP[70], comme en pratique la sécurité routière. En réponse aux observations provisoires de la Cour, le GIP précise que des vidéos de sensibilisation ont été réalisées dans le cadre du programme Conso Mag diffusées sur l'ensemble des chaînes du groupe France TV afin de toucher un large public. Une campagne spécifique a également été effectuée en mai 2020 dont les coûts de production ont été pris en charge par le GIP et la diffusion a été assurée à titre gracieux par le groupe France TV.

Le budget alloué au pôle communication est limité et il n'est pas toujours stabilisé comme en 2020 par exemple, durant la crise sanitaire, où il a servi de variable d'ajustement budgétaire, la gestion de la crise imposant une gestion prioritaire des dépenses incompressibles comme le loyer, le conseil juridique ou encore la maintenance de la plateforme de saisine en ligne.

La contrainte des moyens du GIP pose la question de son modèle fondé sur un financement public et privé, et du développement à terme du financement des partenaires privés, des sociétés membres.

Le directeur du GIP souligne que l'objectif initial d'un financement semi privé est devenu désormais difficile à atteindre. Passer à une phase de développement plus forte nécessite, selon lui, des ressources publiques pérennes. Le GIP envisage par ailleurs la piste d'une évolution législative qui permettrait de différencier la présentation des logos des membres au regard du montant de leur contribution. En réponse aux observations provisoires de la Cour, le GIP indique également réfléchir à une évolution législative visant à inscrire dans la loi les missions du GIP, ce qui pourrait lui permettre de dépendre d'un programme spécifique dans la loi de finances et ainsi pérenniser la partie publique de son financement, voire l'augmenter.

---

[69] cf. marché annuel de participation du GIP ACYMA aux « assises de la sécurité des systèmes d'information ».
[70] Cf. *infra*.

Recommandation n° 5. Mettre en place des ressources financières pérennes pour assurer les missions du GIP ACYMA, en étudiant toutes les solutions publiques et privées. (SGG, SGDSN, ANSSI, GIP)

CONCLUSION INTERMÉDIAIRE

Après une phase de constitution, le GIP semble avoir atteint un palier qui n'est toutefois pas à la hauteur des ambitions initiales, faute de ressources suffisantes. Le groupement a été correctement géré, y compris pendant la crise sanitaire, en respectant son obligation statutaire de maintien à l'équilibre des comptes.

Cette gestion à l'équilibre s'est toutefois effectuée au prix du sacrifice partiel du budget de communication, pourtant primordial pour un organisme dont l'activité s'adresse principalement au grand public et dont le besoin de notoriété est essentiel pour parvenir à le toucher, notamment au titre de ses activités de prévention.

Il apparaît donc nécessaire de mettre en adéquation les ressources financières du groupement avec les missions et les objectifs qui lui ont été confiés par ses membres et par ses tutelles. Pour autant, le développement du GIP cybermalveillance ne peut continuer à s'effectuer sans un soutien administratif plus conséquent, notamment pour ce qui concerne les achats, la gestion des ressources humaines et en particulier des recrutements et sa gestion financière. Ce renforcement devrait s'inscrire dans le cadre d'un suivi plus précis du budget et d'une restitution plus consolidée de l'usage des contributions des membres et des subventions publiques.

3 UNE NÉCESSAIRE MISE EN PERSPECTIVES AVEC LA MONTÉE EN PUISSANCE DE L'ANSSI ET DU CAMPUS CYBER À PARIS-LA DÉFENSE

À ce stade de sa montée en puissance, le modèle du GIP ACYMA est confronté à l'évolution de la sphère de la cybersécurité avec la création d'un campus Cyber et la mise en œuvre d'une nouvelle stratégie française pour la cybersécurité. La question de l'évolution de ses missions se pose, en particulier au regard de la création d'un observatoire de la menace, tout autant que l'adaptation de ses ressources et son positionnement au sein de cette sphère.

3.1 Le concept Cybermalveillance.gouv.fr : jusqu'où étendre le modèle ANSSI ?

L'approche par le haut et par le bas du spectre des menaces cyber s'est révélée pertinente. Elle justifie une réflexion stratégique conjointe entre l'ANSSI, le GIP et ses

membres en raison de l'effort à poursuivre sur la frange centrale des cibles potentielles des cybercriminels qui présente de façon structurelle de véritables fragilités.

3.1.1 Le GIP couvre la partie basse du spectre des cibles potentielles hors du champ d'action de l'ANSSI

En tant qu'autorité nationale de cybersécurité, l'ANSSI conçoit et coordonne la politique nationale en matière de sécurité informatique et définit des normes techniques. Elle joue également un rôle majeur de prévention des attaques informatiques, de détection et d'alerte, et enfin de remédiation. Cependant, un rapport du Sénat de 2020 notait que si « *l'ANSSI intervient auprès d'acteurs de premier plan, […] elle ne peut répondre aux demandes de toutes les entités publiques et privées qui expriment des besoins en matière de cybersécurité.* »

Devant la recrudescence des actes de cybermalveillance ces quatre dernières années, le concept *Cybermalveillance.gouv.fr* s'est avéré pertinent, en couvrant cette frange très fragile que représentent les particuliers, souvent démunis, et les petites entreprises qui n'ont pas les moyens d'investir dans un système d'information protégé. De fait, aujourd'hui l'action de prévention et d'assistance laisse un grand vide au centre du dispositif, c'est-à-dire dans les régions et les territoires, que visent à combler les initiatives prises localement et les mesures qui se mettent progressivement en place, sous la direction de l'ANSSI (voir encadré).

En réponse aux observations provisoires de la Cour, le GIP Acyma indique n'avoir pas cherché à orienter son activité d'assistance vers les plus grosses structures (ETI, grosses collectivités), dans la mesure il a toujours considéré qu'elles disposaient des moyens nécessaires à la remédiation des cyberattaques, que ce soit en propre ou par l'intermédiaire de prestataires déjà identifiés. Le GIP a toutefois produit des contenus de sensibilisation qui ont été relayés par ces structures, dont des ETI et certains OIV/OSE, à leurs collaborateurs.

Le dispositif a par ailleurs cherché dès sa création à s'impliquer dans les territoires où se trouvent la majorité de ses publics, notamment dans la région des Hauts-de-France où sa plateforme a fait l'objet d'une expérimentation en 2017 avant le déploiement national.

La cybersécurité en régions

Depuis 2016, la région Provence-Alpes-Côte d'Azur déploie toute une série de dispositifs d'aide pour accompagner les entreprises dans leur stratégie de digitalisation : *Sud Labs*, *Coach Digital*, etc.

En particulier, la région met à la disposition des entreprises accompagnées des consultants experts sur un large spectre de thématiques numériques liées au contexte de crise :

- ***Webmarketing, communication, présence en ligne :*** communication de crise et comment garder le contact avec sa clientèle grâce aux réseaux sociaux, basculer en e-commerce et booster ses ventes en ligne lorsque le point de vente est fermé, prendre le temps de monter son site internet et créer du contenu ;
- ***Cybersécurité :*** assistance aux entreprises victimes de cyber-attaque, sécurisation de manière ordonnée de la mise en télétravail des collaborateurs, conseil stratégique en cybersécurité ;
- ***Outils métiers et collaboratifs :*** communication entre les collaborateurs, gestion de contacts et de suivi des interactions à distance, partage, stockage, transfert de documents, gestion de projet pour

s'organiser : répartition des tâches, suivi de l'avancement, numérisation, bureautique, simulation de trésorerie. Mais aussi un large éventail de prestations pour préparer la sortie de crise sur toutes les thématiques numériques.

*

Pour faire face à la menace sur les systèmes d'information, la capacité de l'État s'est renforcée tant au niveau central que local. Dans le prolongement d'une réflexion interministérielle sur l'avenir de l'action territoriale en matière de sécurité numérique, l'ANSSI s'est dotée d'un dispositif d'action visant à soutenir le tissu économique et les institutions à l'échelle régionale. Il se traduit par :

- des délégués de l'ANSSI en régions, tous spécialistes de la sécurité du numérique, qui œuvrent en synergie avec les structures et les autorités régionales existantes pour prévenir les incidents et sensibiliser les acteurs locaux du public et du privé aux bonnes pratiques informatiques ;
- un programme de sécurité numérique et économique (SECNUMECO) destiné aux décideurs pour faire face aux risques, accentués par la transformation numérique, qui pèsent de manière indifférenciée sur les structures publiques et privées de toutes tailles et de tous secteurs. SecNumeco comporte quatre volets : se former, appliquer, évaluer, réagir.

Source : Cour des comptes d'après les données Région Sud et ANSSI[71]

Pour l'ANSSI, conjuguer sécurité économique et sécurité numérique « *n'est pas seulement indispensable au bon fonctionnement de chaque organisation : c'est un enjeu de souveraineté nationale* ». En tant qu'enjeu national, la participation de l'État est indispensable, comme le traduit la nouvelle stratégie de la cybersécurité de 2021. Toutefois, le niveau de participation de l'État, à terme, pourrait être appelé à évoluer à l'exemple de la sécurité routière, autre grande politique publique mise en œuvre et dans laquelle nombre d'associations reconnues d'utilité publique sont impliquées, et notamment l'Association Prévention Routière, dont les objectifs visés sont comparables au le concept *Cybermalveillance.gouv.fr* pour le volet prévention-information.

L'association Prévention Routière[72] est régie par la loi de 1901 et reconnue d'utilité publique depuis 1955. Créée en 1949 par les sociétés d'assurance avec l'aide de l'Union routière de France, elle a pour objectif *« d'étudier et mettre en œuvre toutes mesures et encourager toutes initiatives propres à réduire la fréquence et la gravité des accidents de la circulation routière* ». Elle agit au niveau national comme dans les régions et les départements ; elle est membre du Conseil national de la sécurité routière[73] (CNSR) et a été choisie par la Commission européenne pour être le relais français de la charte européenne de la sécurité routière[74].

---

[71] https://www.maregionsud.fr/actualites/detail/la-region-sud-agit-pour-accompagner-les-entreprises-dans-leur-digitalisation ; https://www.ssi.gouv.fr/agence/cybersecurite/action-territoriale/

[72] Source : https://www.preventionroutiere.asso.fr/organisation/

[73] Source : https://www.securite-routiere.gouv.fr/
Le Conseil nationale de la sécurité routière (CNSR) rassemble les principaux acteurs de la sécurité routière, avec leurs compétences et sensibilités respectives, afin qu'ils puissent débattre, échanger et réfléchir pour formuler des propositions concrètes à l'attention du Gouvernement pour inverser la courbe de la mortalité routière.
Décret n°2001-784 du 28 août 2001 portant création du Conseil national de la sécurité routière et modifiant le décret n°75-360 du 15 mai 1975 relatif au comité interministériel de la sécurité routière ; modifié par le décret par le décret n° 2016-1511 du 8 novembre 2016.

[74] Sous l'égide de la Commission européenne, la charte européenne de la sécurité routière, produite en 2004, est la plus grande plateforme dédiée à la sécurité routière. Elle rassemble une communauté de plus de 4 000

Il apparaît donc intéressant d'étudier cette évolution de l'axe prévention, et voire assistance, dans la perspective d'une couverture toujours large du public concerné par le sujet de la cybersécurité.

3.1.2 Une stratégie reste à définir pour l'après 2022

La *Stratégie nationale pour la cybersécurité* de février 2021 entend « *apporter une réponse spécifique pour les territoires* » en allouant dans le cadre de France Relance[75] un budget de 136 millions d'euros sur la période 2021-2022 – dont le GIP bénéficie à hauteur de 691 000 euros, soit 0,6 % du montant total attribué à l'ANSSI (cf. chapitre 2) - piloté par l'ANSSI et destiné à la cybersécurisation des territoires[76]. Cette stratégie met également en lumière la prévention au titre de « [la] *sensibilisation et* [de l']*hygiène numérique* » en présentant *Cybermalveillance.gouv.fr* comme « *une plateforme au service du plus grand nombre.* »

Au moment où l'ANSSI renforce son réseau régional et développe de nouvelles capacités (voir encadré *supra*), le GIP ACYMA, avec son réseau de partenaires institutionnels et privés et de prestataires labellisés *ExpertCyber* qu'il continue d'étendre, reste un élément clé du triptyque « prévention-assistance-anticipation » au niveau national. La question se pose donc de son implication dans les *Computer Security Incident Response Team*[77] (CSIRT) régionaux, au sein desquels l'ANSSI va développer des compétences d'accueil, d'information et de formation.

Enfin, compte tenu de l'aspect stratégique que revêt la cybersécurité pour la résilience des structures de l'État aussi bien que de l'économie et de la société dans son ensemble, la part de ressources publiques pérennes à consacrer à l'évolution du concept *Cybermalveillance.gouv.fr* mérite d'être appréciée à sa juste valeur.

Une réflexion devrait être menée sur l'évolution du concept *Cybermalveillance.gouv.fr* au-delà de 2022 et de la mise en œuvre du plan France Relance. Cette réflexion pourrait déboucher sur une nouvelle stratégie pour le GIP ACYMA, intégrant son rôle et son positionnement dans la sphère cybersécurité, y compris dans les régions en coopération avec les CSIRT ; son implication dans la formation des personnes et des structures professionnelles ou associatives au niveau local ; et bien évidemment sa fonction de relais vers des prestataires de service pour la remédiation des systèmes d'information ayant subi une attaque ou l'aide à personne ayant été victime d'une arnaque informatique.

---

organismes publics et privés (associations, entreprises, collectivités locales, institutions de recherche, universités…) de toute l'Union européenne, qui s'engagent tous à mener des actions de sécurité routière ainsi qu'à partager leurs bonnes pratiques et leur expertise. (*Source : https://www.preventionroutiere.asso.fr/charte-europeenne-de-securite-routiere-european-road-safety-charter/)*

[75] Le gouvernement a lancé, le 3 septembre 2020, un plan de relance historique de 100 milliards d'euros pour redresser l'économie et faire la **«** France de demain ». Inscrit dans la continuité des mesures de soutien aux entreprises et salariés lancées dès le début de la crise de la Covid-19, ce plan vise à transformer l'économie et créer de nouveaux l'emploi. Il repose sur trois piliers : l'écologie, la compétitivité et la cohésion.
Source : Ministère de l'économie, des finances et de la relance
https://www.economie.gouv.fr/presentation-plan-relance

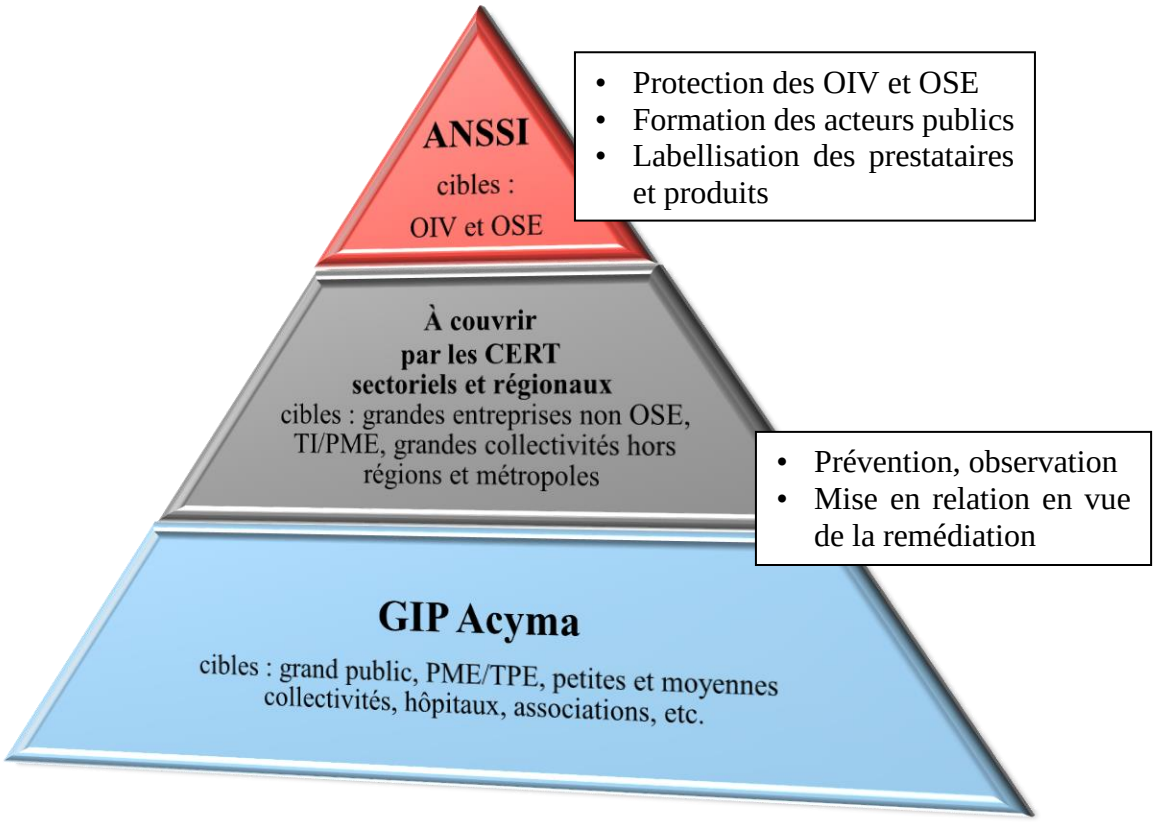
[76] *Stratégie nationale pour la cybersécurité* de février 2021, p.16.

[77] Cf. note de bas de page n°64.

3.1.3 Une réflexion sur l'organisation doit être menée en lien avec la revue stratégique des missions

La structure de groupement d'intérêt public a d'abord été pensée dans une logique de financement, avant même de répondre à la nécessité d'échanges entre les différents acteurs publics et privés du secteur. La lutte contre la cybermalveillance étant devenue entretemps une véritable politique publique, il est nécessaire de réexaminer la pertinence de l'organisation actuelle.

Schéma n° 2 : La couverture du spectre de la menace par les différents acteurs



Source : Cour des comptes à partir des entretiens ANSSI et GIP

Trois types d'organisation alternative, en fonction de la stratégie de couverture retenue, pourraient être adoptés :

- transformer le GIP en structure associative ;
- réintégrer la protection du bas du spectre au sein de l'ANSSI ;
- adopter un modèle mixte dans lequel l'ANSSI définirait la stratégie, animerait une structure de concertation sur le modèle du comité national de la sécurité routière ou du conseil national du numérique, et laisserait le soin à une fondation ou à une association émanant du secteur privé la tâche de prévention et de mise en relation avec les prestataires de remédiation.

En fonction des choix qui devront être exposés dans le plan stratégique du GIP Acyma, l'organisation de la structure chargée de mettre en œuvre la stratégie retenue devra être explicitée, une quatrième option étant de conserver la structure actuelle en l'état en précisant la répartition des rôles entre le GIP et l'ANSSI[78] pour une meilleure couverture du milieu du spectre.

Recommandation n° 6. Élaborer un plan stratégique à cinq ans pour l'évolution du GIP ACYMA après 2022, en cohérence avec la stratégie nationale de cybersécurité. (SGG, SGDSN, ANSSI, GIP)

3.2 Un intérêt limité de l'installation du GIP au sein du Campus cyber

La création d'un campus Cyber regroupant les principaux acteurs publics et privés de la communauté cyber est l'un des éléments de la stratégie de cyberdéfense annoncée le 18 février 2021 par le gouvernement[79] issue de la revue de cyberdéfense de 2018. Dans ce contexte le GIP avait envisagé de s'y installer, notamment dans le but de construire l'observatoire de la menace, avant d'y renoncer en raison des coûts excessifs, au regard des ressources, de l'installation de l'ensemble du GIP.

3.2.1 La participation au campus Cyber permettrait d'accélérer la réalisation de l'observatoire de la menace

3.2.1.1 Le campus Cyber fait partie intégrante de la nouvelle stratégie de cyberdéfense française

Le campus Cyber a été envisagé comme un noyau central de la politique de la sécurité numérique française, rassemblant aussi bien des acteurs publics (ANSSI, ministère de l'intérieur, ministère des armées et INRIA) que privés tels que des startups, des industriels[80], des institutionnels, des entités de formation et de la recherche ou des associations.

La direction du projet a été confiée à M. Michel Van Den Berghe, directeur général d'Orange Cyberdéfense, après le cadrage de la réunion interministérielle (RIM) du 24 janvier 2020, à laquelle ont participé l'ANSSI et la direction générale des entreprises (DGE) du ministère de l'économie. Une nouvelle RIM a eu lieu le 2 avril 2020 pour consolider la participation des acteurs publics à ce projet pour laquelle certains obstacles budgétaires restaient

[78] La convention d'objectif de la subvention exceptionnelle France relance au profit du GIP en 2021 précise, dans l'axe 2, que le GIP doit développer la coopération avec les CIRST régionaux, notamment *« accompagner les CIRST régionaux en construction pour assoir l'offre de chacun en fonction de son périmètre et coordonner les actions »* [annexe 1 de la convention en date de 2021].
[79] Dossier de presse du 18 février 2021, *Cybersécurité, faire face à la menace : la stratégie française*.
[80] Notamment les grands industriels Capgemini, Atos, Sopra Steria, Orange Cyber Défense, Thalès, Wavestone, Airbus.

à lever. L'inauguration du site de La défense à Paris initialement prévue fin 2021, a eu lieu le 15 février 2022.

3.2.1.2 Les coûts engendrés par une installation complète sur le site de La Défense paraissent disproportionnés au regard de la taille de l'organisme

L'installation complète du GIP au sein du campus Cyber semble démesurée par rapport à son budget actuel de fonctionnement. Le groupement occupe actuellement des locaux situés rue Bouchardon, dans le X^{e} arrondissement de Paris alors que le futur campus Cyber occupera une tour de 12 étages de La Défense, dont les différents espaces de bureau homogènes, appelés « pétales », sont d'une surface de 1 020 m^2. Le GIP considère qu'une surface de 360 m^2, soit moins d'un demi-pétale, serait nécessaire s'il devait y loger l'ensemble de son activité

Tableau n° 12 : Principaux ratios immobiliers du GIP

	Rue Bouchardon	La Défense
Total m^2	375	360
Loyer annuel (en euros)	173 000	260 000
Prix annuel au m^2 (en euros)	461	722
Salariés	13	16
Ratio salarié/m^2	29	23

Source : Cour des comptes à partir des données fournies par le GIP

Les surfaces actuelles ou projetées par agent apparaissent confortables, même en tenant compte de l'accroissement prévisible de l'effectif du GIP. La norme Afnor NF X 35-102[81] recommande en effet un espace minimum de travail de 10 m² par personne et de 15 m² par personne dans un espace bruyant. La direction immobilière de l'État (DIE) vise pour sa part un ratio SUN[82]/poste de travail de 12 m^2 au sein des administrations publiques du périmètre étatique.

Le GIP a envisagé plusieurs hypothèses,

- détachement d'un seul salarié sur place dès l'ouverture ;
- déménagement de l'ensemble de l'entité dès l'ouverture ;
- déménagement partiel avec maintien d'une partie de l'équipe sur le site historique de la rue Bouchardon.

Aucune ne semblant totalement satisfaisante pour des raisons de ressources humaines, d'organisation et surtout de coût, le groupement a décidé d'armer uniquement une cellule de liaison avec un seul salarié, chargé de la réalisation de l'observatoire de la menace, qui pourrait

[81] La norme NF X35-102 définit les caractéristiques des locaux de travail à usage de bureaux intégrant des équipements bureautiques. Il s'agit d'une norme volontaire de l'AFNOR c'est-à-dire d'un cadre de référence non obligatoire, que l'entreprise peut choisir ou non d'appliquer.
[82] La surface utile nette correspond aux surfaces de bureau, de réunion et des annexes de travail.

être hébergé par l'ANSSI ou par l'un des partenaires ou membres du GIP présents sur le campus.

Cette solution apparaît raisonnable au regard des prix élevés du m^2 au sein du campus cyber, qui conduiraient à augmenter de 50 % les coûts immobiliers alors qu'une seule de ses activités semble ne pas pouvoir se passer d'une présence dans ce lieu.

Le GIP pourrait réexaminer cette position en fonction des ressources du groupement et de sa montée en puissance, la participation au campus Cyber pouvant être un outil d'influence et de mise en relation avec les différents acteurs de l'univers de cybersécurité.

En réponse aux observations provisoires de la Cour, le SGDSN indique que l'ANSSI mettra à disposition du GIP ACYMA quatre postes de travail physiques au sein du Campus Cyber. Il précise que *« dans le cadre d'une bonne évaluation des coûts de fonctionnement, […] cet hébergement sera évalué financièrement et intégré dans la dotation de l'ANSSI au dispositif. »*

Le campus Cyber

Lancé par la revue stratégique de cyberdéfense de février 2018 qui recommandait d'élaborer une programmation spécifique des moyens publics consacrés à la cyberdéfense, le projet de campus Cyber s'est développé au cours de l'année 2020. Il vise à permettre à l'ensemble des acteurs de la cybersécurité de travailler conjointement sur des projets d'intérêts communs.

Au sein du campus Cyber, l'ANSSI, en tant qu'autorité nationale de cybersécurité, aura pour mission d'insuffler auprès de ses partenaires publics et privés des projets visant à assurer la montée en compétence et la performance de la France en matière cyber.

Le campus Cyber a comme ambition de devenir le lieu de référence de l'écosystème français de cybersécurité. Plus de 70 acteurs de la sécurité numérique (startups, industriels, institutionnels, entités de formation et de la recherche, associations) ont fait part de leur intérêt pour devenir membres du campus. Les acteurs privés occuperont une majorité des espaces avec des grands groupes de la cybersécurité et du numérique (*Capgemini, Atos, Sopra Steria, Orange Cyberdéfense, Thalès, Wavestone, Airbus*, etc.) et des acteurs de taille plus modeste (*Gatewatcher, Yes we Hack, Egerie*, etc.). Une diversité d'acteurs publics sera également présente sur le campus Cyber avec, outre l'ANSSI, le ministère de l'intérieur, le ministère des armées et l'INRIA. Des dispositifs d'accompagnement de l'innovation au travers de plateau-projets et d'incubateur de start-up doivent également être mis en place avec le soutien de l'État.

Le projet immobilier est structuré autour d'un partenariat privé-public, la participation des acteurs privés au capital de la SAS sera majoritaire à hauteur de 51 %, celle de l'État interviendra en fonds propres à hauteur de 49 % pris en charge par l'agence des participations de l'État (APE). La surface effective de l'implantation de l'ANSSI s'élèvera à 1 698 m^2 divisée en trois zones à des usages distincts :

- une zone « formation » de 622 m^2 destinée au centre de formation de l'ANSSI (CFSSI) qui comportera principalement des salles de cours. Le CFSSI, actuellement localisé à la Tour Mercure (15^e arrondissement) sur une surface de 300 m^2, doublerait ainsi sa capacité d'accueil ;
- une zone « expertise » de 517 m^2 qui comportera 30 postes de travail permettant la conduite de projets collaboratifs avec les membres du campus ;
- une zone « écosystème » de 559 m^2 qui comportera 48 postes de travail composés de bureaux et d'espaces de *co-working* favorisant les interactions au sein des réseaux opérationnels des CSIRT, pour les missions d'orientation industrielle et d'accompagnement des acteurs en matière de cybersécurité.

L'une des caractéristiques du Campus Cyber est la mise à disposition d'espaces communs pour mener des projets collaboratifs. Elle se traduit par une évaluation particulière de la surface pour établir le loyer. Cette surface appelée quote-part parties communes (QPPC) s'élèvera à 2 234 m^2 pour l'ANSSI, représentant 11 581 056 € de loyer TTC sur six ans (la durée du bail négociée par la DIE auprès de la SAS Campus Cyber et le bailleur étant de six ans).

Les coûts d'aménagement standards proposés par la SAS Campus Cyber pour la surface de l'ANSSI s'élèvent à 1 400 432 € HT soit 1 680 515 € TTC.

Source : Cour des comptes d'après les données de l'ANSSI

3.2.2 Le GIP contributeur ou maître d'ouvrage de l'observatoire de la menace ?

Le manque de statistiques précises et de données d'environnement sur le grand public est constaté par tous les acteurs et notamment par les acteurs judiciaires et ceux des forces de sécurité. Une meilleure visibilité de la menace et de ses implications permettrait à la fois d'anticiper les grandes tendances, d'adapter les moyens consacrés aux enjeux et de mieux mesurer l'efficacité des politiques adoptées. Le GIP ayant un accès privilégié au grand public, paraît bien placé pour collecter des données sur le sujet, identifier les tendances naissantes et interpréter les signaux faibles.

Toutefois, la tâche paraît quelque peu ambitieuse au regard de l'effectif du GIP et de l'étendue de ses autres missions, dans la mesure où un tel observatoire requiert à la fois des compétences techniques, administratives et mêmes géopolitiques pour identifier les différents acteurs, les types d'attaques, la réglementation nationale et internationale, le rôle des acteurs gouvernementaux et des associations, etc.

Une partie de ces missions est actuellement assurée par la sous-direction stratégie de l'ANSSI et par chacun des acteurs concernés dans le continuum de sécurité, mais les informations, éléments d'intérêt et statistiques ne sont que partiellement partagés. L'ANSSI informe régulièrement ses correspondants et le grand public des différentes menaces, donne quelques éléments de contexte dans son rapport annuel ou dans ses différents documents publics, tandis que les autres acteurs ont tendance à n'exporter que ce qui relève de leur activité propre.

Dans ce contexte, la mise en réseau des principaux acteurs apparaît comme un levier important dans la mise en place de l'observatoire, et nécessiterait très probablement une présence permanente du GIP au sein du campus Cyber. Il est toutefois permis de s'interroger sur la capacité du GIP à fédérer l'ensemble des acteurs, ainsi que sur la légitimité du groupement, auprès des autres acteurs, pour conduire seul une telle mission. Une répartition des rôles avec l'ANSSI et au moins une coopération étroite sur le sujet restent indispensables. Le fait que l'ANSSI envisage d'installer dans le campus Cyber certains des éléments de sa sous-direction stratégie apparaît de fait positif pour l'avenir du projet.

À l'aune des ambitions affichées au niveau national, après une réflexion conjointe entre toutes les parties prenantes à la construction de cet observatoire de la menace, un plan de montée en puissance doit être formalisé et accompagné d'un processus clair quant aux responsabilités dévolues à chaque partie et sur le pilotage de cette « structure ».

En réponse aux observations provisoires de la Cour, le SGDSN considère que l'ANSSI devrait piloter l'élaboration et l'animation de l'observatoire, auquel le GIP devra contribuer. Le

ministère de l'intérieur, quant à lui, confirme que la mise en place de cet observatoire est suivie au sein du ministère, dans la mesure où le dispositif devra également associer la DPSIS et le service à compétence nationale cyber, commun à la police et la gendarmerie nationales. Il appartiendra au SGDSN de clarifier formellement le positionnement de l'ANSSI dans la mise en place de cet observatoire de la menace.

Recommandation n° 7. Mettre en place l'observatoire de la menace cyber, en fixer les objectifs, la répartition des responsabilités et les modalités de fonctionnement. (SGG, SGDSN, ministère de l'intérieur, ministère de la justice, ANSSI, GIP)

3.3 Une nécessaire adaptation du GIP et de son modèle économique

3.3.1 Les ressources permanentes actuelles ne suffisent pas à assurer le financement des ambitions du GIP

S'agissant d'un organisme destiné à communiquer au grand public pour assurer ses missions, notamment de prévention, la construction d'une notoriété suffisante paraît indispensable et passe par des actions de communication plus massives.

3.3.1.1 La cible grand public du groupement implique une stratégie de communication ambitieuse et coûteuse

Les différentes cibles du GIP, particuliers, PME, collectivités locales de taille petite et moyenne, établissements hospitaliers, associations, etc. ne peuvent être touchées qu'au moyen de médias grand public sous la forme par exemple de publicité radiodiffusée. Le modèle évoqué par le GIP est celui de la prévention routière, qui fait l'objet de campagnes radio et télévision de longue date. Selon le GIP, une évaluation sommaire par le service d'information du gouvernement (SIG) établissait qu'un budget annuel de quatre millions d'euros serait nécessaire, *a minima*, pour assurer de telles campagnes, se répartissant entre 600 000 euros pour la création et 3,4 millions d'euros pour la diffusion.

La subvention exceptionnelle de 691 000 € accordée en 2021 dans le cadre du plan France relance ne prévoit pas de budget destiné à une vaste campagne de sensibilisation comme le souhaiterait le pôle communication en raison du coût élevé de sa diffusion. Le pôle communication est ainsi contraint de trouver de nouveaux moyens de communication pour diffuser massivement de l'information à un faible coût, ce qui limite le déploiement de ses actions.

Selon la Cour, dans sa récente évaluation de la politique publique de sécurité routière[83] le coût de la démarche de communication de la délégation à la sécurité routière (DSR) du ministère de l'intérieur entre 2008 et 2019 était de 18 millions d'euros annuels en moyenne.

Les seules dépenses du programme 207, « sécurité et éducation routière » au titre de la communication grand public s'élevaient à 7,8 millions d'euros de crédits de paiement en 2020, dont 6,91 millions affectés aux seules « campagnes nationales de mobilisation »[84]. Ces dépenses ne représentent d'ailleurs qu'une fraction du total, d'autres ministères participant à la communication grand public sur leurs propres programmes.

3.3.1.2 La progression des ressources financières n'est pas forcément pérenne

D'autre part, l'engagement dans la création d'un réseau régional de centres de lutte contre les attaques cybermalveillantes (CSIRT régionaux) va nécessiter une animation de la part du GIP, qui devra donc y consacrer des ressources supplémentaires. L'ANSSI a annoncé consacrer une partie des fonds qui lui sont dévolus par le plan de relance au financement de la mise en place de ces centres et a accordé une subvention de 120 000 euros pour l'année 2021 au GIP pour développer la coopération avec les CSIRT régionaux, mais ce ne sont pas des ressources permanentes. Cette subvention exceptionnelle qui lui a permis de boucler son budget 2021 n'est ni pérenne, ni même à la hauteur des enjeux de notoriété du groupement.

3.3.2 De nouvelles pistes de financement pourraient être explorées

Il est donc nécessaire d'envisager d'autres moyens de financement pour le GIP, le recours aux seules contributions des membres n'étant manifestement pas suffisant. Celles-ci n'étant pas des cotisations, elles peuvent varier d'une année à l'autre dans les limites fixées par la convention sans que le groupement puisse nécessairement le prévoir. Le non-versement de la contribution ne peut constituer une clause de suspension, que si l'assemblée générale en décide ainsi, sur proposition du conseil d'administration. Une telle décision prive seulement le membre concerné de sa voix délibérative aux instances de gouvernance.

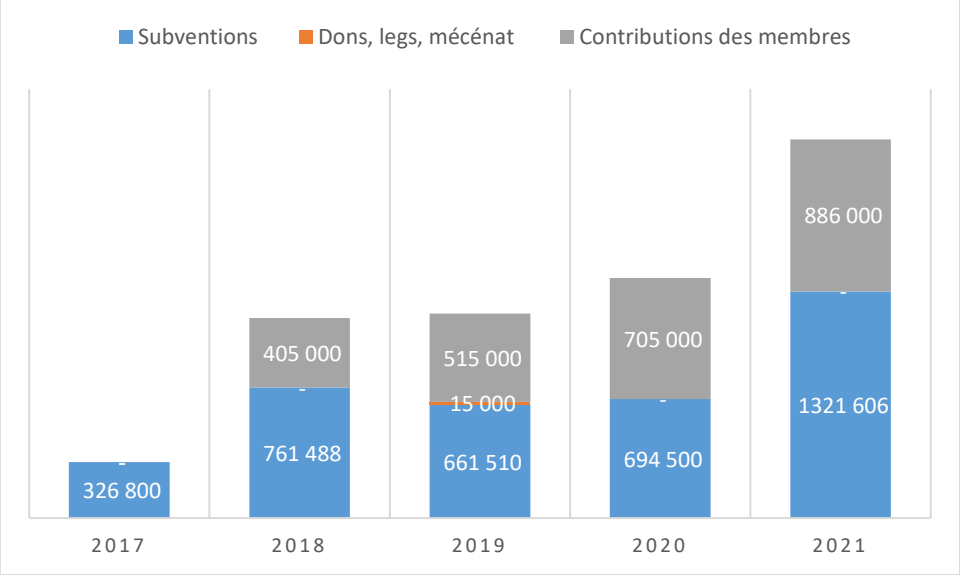
3.3.2.1 Élargir le cercle des membres ou augmenter leurs contributions ?

Les contributions des membres des quatre collèges ne suffisent pas à assurer le financement des objectifs du GIP. Elles ne représentent aujourd'hui qu'un peu moins de la moitié des ressources du groupement, sans avoir jamais été très sensiblement supérieures à la moitié comme le montre le graphique ci-après.

---

[83] *Évaluation de la politique publique de sécurité routière*, rapport public thématique, juin 2021.
[84] Projet annuel de performance annexé à la loi de finances pour 2020, mission sécurités.

Graphique n° 7 : Répartition des ressources financières du groupement



Source : Cour des comptes à partir des données du GIP Acyma.

Le GIP Cybermalveillance fonde sa stratégie de développement sur la subvention versée par l'ANSSI mais également, compte tenu de son statut juridique, sur les contributions financières des membres. Celles-ci ont progressé sur la période 2018-2020 de 77 % mais le GIP Cybermalveillance est conscient des limites et de la fragilité d'un mode de financement privé non pérenne nécessitant un suivi permanent et des ressources humaines suffisantes en interne pour relancer et animer ce réseau.

En outre, le montant des contributions des membres apparaît décorrélé de leur capacité contributive. De grandes entreprises du numérique, notamment celles des grands acteurs internationaux de l'internet ou de l'édition de logiciels, contribuent au même niveau que des PME. Il pourrait donc être judicieux d'inciter ces membres à apporter une contribution plus en rapport avec leur surface financière en leur assurant éventuellement de meilleures retombées en termes d'image, mais ceci est rendu difficile, voire impossible, par le principe d'égalité entre les membres, indépendamment du montant de leur contribution.

Une autre possibilité est d'élargir le cercle des contributeurs, notamment en y intégrant les autres bénéficiaires et partenaires que sont les grandes collectivités locales comme les régions et les associations les représentant (association des maires de France, associations des régions notamment) ou encore les établissements hospitaliers et les différents groupements (Assistance publique des hôpitaux de Paris, hospices civils de Lyon, APHM, etc.). Les compagnies d'assurance et les banques, qui pâtissent dans leur activité des actes de cybermalveillance, pourraient également être utilement mises à contribution.

Il serait toutefois illusoire de penser que ces seules ressources seront suffisantes pour assurer le doublement du budget actuel. En tout état de cause, la recherche de financements nécessitera de renforcer l'effectif destiné à les collecter et pourrait conduire, à terme, au recrutement d'un salarié spécialement chargé de la recherche de nouveaux partenariats financiers.

En réponse aux observations provisoires de la Cour, le groupement indique que les compagnies d'assurance et les banques ont bien été prospectées. Si certains assureurs et la fédération française de l'assurance (FFA), membre fondateur, ont souhaité participer aux travaux et contribuer au GIP, seule la banque Neuflize OBC est membre du GIP et contribue à son activité. Les autres banques, tout comme la fédération bancaire française, n'ont jusqu'à présent pas encore adhéré au GIP pour le soutenir dans ses missions, même si elles utilisent déjà, pour certaines, les productions du GIP pour leurs actions de sensibilisation.

La prospection en direction des banques et organismes d'assurance doit être poursuivie et renforcée, celles-ci ayant parfois tendance à privilégier de manière excessive le retour sur investissement des actions de prévention sur la responsabilité sociale et environnementale à l'égard de leurs clients.

3.3.2.2 Abandonner la philosophie du tout gratuit

Le GIP fournit de nombreuses prestations de formation et d'homologation, notamment des entreprises chargées de la remédiation aux actes de cybermalveillance qu'elle met en relation avec les usagers victimes par l'intermédiaire de son site web et de la plateforme de référencement qui y est associée sans aucune contrepartie sous quelque forme que ce soit.

Il paraît difficile de demander aux particuliers ou aux petites organisations ou collectivités de contribuer à cette mise en relation. Mais la perception d'une redevance à l'homologation, appuyée par un texte la rendant au besoin obligatoire pourrait être envisagée.

Si la totale gratuité, commune à l'ANSSI, peut se justifier lors d'une phase d'« évangélisation » elle apparaît moins légitime au long cours.

3.3.2.3 Trouver des sources alternatives de financement par le recours à des subventions publiques ou à la générosité publique

D'autres sources de financement restent donc à trouver, si le GIP veut remplir les objectifs qu'il s'est assigné. L'une des pistes pourrait être l'augmentation des subventions publiques, en diversifiant éventuellement les ministères financeurs, voire les collectivités territoriales intéressées, mais la part du secteur public dans le total des ressources du groupement est déjà relativement élevée. En outre, privilégier ce mode de financement reviendrait à remettre en question de fait l'objectif initial de ce GIP d'associer financements publics et privés.

Une autre piste envisagée par le GIP serait le recours à l'appel public à la générosité, notamment en direction des entreprises et du mécénat, qui offrirait un avantage fiscal supplémentaire aux donateurs et pourrait ainsi se révéler plus attirant pour les entreprises partenaires que la simple contribution. Le recours à la générosité publique comme moyen de diversification des sources de financement du GIP ACYMA participe de la réflexion menée en interne sur le déploiement de financement privé inhérent au statut juridique du GIP (financement public et privé). Les difficultés tant humaines que conjoncturelles rencontrées par le GIP pour accroître ses ressources privées posent plus largement la question de son statut juridique et de l'opportunité à conserver ou non le statut de GIP.

Dans le prolongement de la réflexion menée sur la diversification de ses sources de financement, le GIP Cybermalveillance a déposé le 11 mai 2020 une demande de rescrit auprès de la direction générale des finances publiques relative à la mise en œuvre de la garantie prévue à l'article L.80 C du livre des procédures fiscales, au profit d'organismes recevant des dons. Dans sa demande, le GIP ACYMA précise qu'il *« assure la gestion d'un service public administratif dont les bénéficiaires sont à la fois l'ensemble des particuliers, les opérateurs économiques, les organisations professionnelles et associatives, les établissements publics locaux, sur tout le territoire national […] qu'il assure la gestion d'activités d'intérêt général à but non lucratif […] qu'il n'intervient pas auprès d'un cercle restreint de personnes et ne facture pas de prestations »*. Il mentionne également que les projets pour lesquels le GIP *« entend rechercher des financements sous couvert de dons éligibles aux articles 200 et 238 bis du CGI sont des projets à caractère social, éducatif et scientifique relevant de missions d'intérêt général du GIP »*.

La description des projets participe de la contribution du GIP ACYMA aux actions de sensibilisation et d'accompagnement dans l'éducation au numérique des utilisateurs « exclus », de l'accompagnement de l'enseignement du numérique sous l'angle de la sécurité auprès des enfants et des adolescents, d'actions à mener auprès des familles en lançant des campagnes médiatiques de grande ampleur sur le modèle de celles de la sécurité routière pour toucher l'ensemble des foyers et des publics. Figure également parmi ces projets la création d'un observatoire de la menace en France pour mieux la comprendre, l'anticiper et la combattre et nécessitant un accompagnement financier conséquent (voir *supra*).

L'action de mécénat peut donc être désormais mise en place par le GIP ACYMA. Il a cependant été décidé en 2021 de la reporter compte tenu de la situation financière dégradée des sociétés susceptibles de devenir membres et fragilisées par la crise sanitaire, et par la difficulté du GIP à mobiliser en interne les moyens humains pour l'animer et la suivre.

Enfin, il pourrait être envisagé de financer le groupement au moyen d'amendes perçues sur les failles de sécurité par les éditeurs concernés ou sur les manquements à la sécurité constatés dans le respect des règles du RGPD, même si la mise en œuvre opérationnelle de ce type d'amende administrative serait quelque peu délicate en l'état, le GIP n'étant pas une autorité administrative indépendante et ne pouvant y procéder de sa propre initiative.

CONCLUSION INTERMÉDIAIRE

Les missions assignées au GIP par la puissance publique au travers de la stratégie nationale de cybersécurité de 2015 apparaissent à la fois suffisamment importantes pour les publics actuellement peu ou pas couverts par l'opérateur du « haut du spectre », l'ANSSI et ambitieuses au regard des objectifs annoncés en février 2021 par le gouvernement pour qu'elles fassent l'objet d'une planification stratégique à cinq ans, afin de détailler les moyens employés pour y parvenir, ainsi que les ressources qui pourront lui être consacrées.

L'organisation du groupement devra tenir compte des choix stratégiques à mettre en œuvre à l'issue de la conception de ce plan en choisissant parmi les différents modes possibles, conservation du statut existant, réintégration des missions au sein de l'ANSSI, délégation à une fondation ou à une association, système mixte.

L'installation du groupement au sein du cyber campus de La Défense, un instant envisagée, ne devrait se faire que de manière symbolique, par l'occupation possible d'un bureau de passage, pris éventuellement au besoin sur la surface occupée par l'ANSSI, par un agent de liaison. Le coût du loyer au m^2 paraît rédhibitoire pour l'installation de l'ensemble du GIP et présenterait peu d'intérêt pour l'ensemble de son activité en dehors des nécessaires échanges avec la communauté cyber sur la construction d'un observatoire de la menace, demandée par tous les acteurs.

En tout état de cause, les ressources financières apparaissent insuffisantes pour réaliser les deux objectifs de prévention et d'assistance au cœur des missions du groupement, et ce malgré un bilan positif de mise en place d'une plateforme internet d'assistance et de saisie en ligne des incidents de cybersécurité. Faute de moyens supplémentaires, il serait nécessaire de revoir les ambitions à la baisse dans un contexte de croissance soutenue de la menace, souvent entretenue par des États ou des groupes paraétatiques.

Toutefois, une augmentation des ressources ne pourrait se produire sans une formulation claire des objectifs à atteindre et des indicateurs permettant de s'assurer de leur réalisation (taux de pénétration dans le grand public, réalisation de CERT régionaux et sectoriels, nombre de prestataires référencés, taux de couverture régionale et sectorielle, etc.) et d'un phasage précis de leur mise en place.

ANNEXES

Annexe n° 1. Sigles utilisés

ACYMA : assistance aux victimes d'actes de cybermalveillance

ANSSI : agence nationale de la sécurité des systèmes d'information

BEFTI : brigade d'enquête sur les fraudes aux techniques de l'information de la préfecture de police de Paris

BLCC ou BL2C : brigade de lutte contre la cybercriminalité de la préfecture de police de Paris

C3N : centre de lutte contre les criminalités numériques du service central du renseignement criminel de la gendarmerie nationale

C4 : centre de coordination des crises cyber

CERT : *Computer Emergency Response Team*, synonyme de CSIRT

CESDH : convention européenne de sauvegarde des droits de l'homme

CESIN : club des experts de la sécurité de l'information et du numérique

CGI : code général des impôts

CNSR : conseil national de la sécurité routière

C-NTECH : correspondant des enquêteurs technologies numériques (gendarmerie nationale)

COE : *Council of Europe* (Conseil de l'Europe)

ComCyberGend : commandement de la gendarmerie dans le cyberespace

CSIRT : *Computer Security Incident Response Team*, synonyme de CERT

CSNP : commission supérieure du numérique et des postes

DCPJ : direction centrale de la police judiciaire

DGSI : direction générale de la sécurité intérieure

Ddos : *Distributed Denial of Service*

DPSIS : délégation ministérielle aux partenariats, aux stratégies et aux innovations de sécurité

ENISA : *European Union Agency for Cybersecurity*

ETI : entreprise de taille intermédiaire

FSN : fournisseur de services numériques

GIP : groupement d'intérêt public

JIRS : juridictions inter-régionales spécialisées

INC : institut national de la consommation

INRIA : institut national de recherche en informatique et en automatique

JUNALCO : juridiction nationale de lutte contre la criminalité organisée

LBSI : Livre blanc de la sécurité intérieure

MEDEF : mouvement des entreprises de France

NCSC : *National Cyber Security Center*

NIS : *Network and Information Systems Security* (directive UE)

NTECH : technologies numériques

OCLCTIC : office central de lutte contre la criminalité liée aux technologies de l'information et de la communication ; service à compétence nationale au sein de la SDLC

OIV : opérateur d'importance vitale

OSE : opérateur de services essentiels

PHAROS : plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements

PJGN : pôle judiciaire de la gendarmerie nationale

PME : petites et moyennes entreprises

PNLC : pôle national de lutte contre les cybermenaces (PNLC) de la gendarmerie nationale

PSSIE : politique de sécurité des systèmes d'information de l'État

RGPD : règlement général de protection des données

SCN : service à compétence nationale

SDLC : sous-direction de la lutte contre la cybercriminalité de la direction centrale de la police judiciaire

SECNUMECO : sécurité numérique et économique

SGDSN : secrétariat général de la défense et de la sécurité nationale

SIG : service d'information du gouvernement

SSD : *Solid State Drive* (support de stockage informatique sans élément mécanique à base de mémoire flash)

SSI : sécurité des systèmes d'information

THESEE : traitement harmonisé des enquêtes et signalements pour les e-escroqueries

TPE : très petite entreprise

URL : *Unique Ressource Locator* (exemples : http://, ftp://, etc.)

Annexe n° 2. Définitions

Ces définitions tirées de celles fournies par l'agence nationale de sécurité des systèmes d'information (ANSSI), complétée par les définitions applicables au ministère des armées ou utilisées par lui, notamment dans un contexte opérationnel[85].

Cyberespace

Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numérique.

Cyberdéfense

Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels.

Cybersécurité

État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace et susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessible. L'ANSSI précise que la cybersécurité « *fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense* ».

Cybercriminalité

Elle est constituée des « *actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible* ».

Cyberattaque

« *Action volontaire, offensive et malveillante, menée au travers du cyberespace et destiné à provoquer un dommage (en disponibilité, intégrité ou confidentialité) aux informations ou aux systèmes qui les traitent, pouvant ainsi nuire aux activités dont ils sont le support* » selon le glossaire interarmées de terminologie opérationnelle (GIATO),

Cyberrésilience

Capacité d'un système d'information à résister à une panne ou une cyberattaque et à revenir à son état initial après l'incident ou, du moins, à un état de fonctionnement et de sécurité satisfaisant.

[85] Vocabulaire de la défense : cyberdéfense (liste de termes, expressions et définitions adoptés), *JORF n° 0219 du 19 septembre 2017, et glossaire interarmées de terminologie opérationnelle.*

Lutte informatique défensive (LID)

Dans le cadre des opérations dans le cyberespace, action consistant à surveiller, analyser, détecter et réagir face à des attaques, intrusions ou perturbations qui pourraient compromettre, paralyser ou détruire les systèmes, réseaux et données.

Lutte informatique offensive (LIO)

Dans le cadre des opérations dans le cyberespace, action non physique entreprise dans le cyberespace contre des systèmes d'information ou des données pour les perturber, les modifier, les dégrader ou les détruire.

Annexe n° 3. Les différents types de réseaux[86] et de cybermenaces[87].

Sur les forums cybercriminels, les notions de *deepweb* et de *darkweb* sont souvent utilisées l'une pour l'autre indifféremment sans que cela ne pose de problème. Pour décrire la différence entre ces deux concepts, l'image d'un iceberg avec au sommet le web surfacique (le web « classique ») et, sous l'eau, le *deepweb* puis le *darkweb* fait référence. Il faut être prudent avec cette illustration car elle est imparfaite : elle suppose une forme de hiérarchie ou de gradation entre les concepts qui ne correspond pas à la réalité. De nombreux experts considèrent d'ailleurs que le *darkweb* en tant que tel n'existe pas et qu'il ne s'agit en fait que d'une fraction du web. Il n'y a donc pas lieu de le traiter différemment.

Darknet

Un *darknet* est un réseau qui pourrait être qualifié de parallèle et qui ne serait accessible qu'à l'aide d'outils spécifiques. Les plus connus sont Tor, i2p et Freenet, mais il en existe beaucoup d'autres. Ces réseaux sont dits « superposés » car ils reposent sur un autre pour fonctionner, internet en l'occurrence. Il n'y a donc pas de *darknet* sans internet.

Darkweb

Le *darkweb*, ou « web clandestin », serait le web non indexé et non accessible par des moyens standard. Le terme « *darkweb* » est aussi généralement utilisé pour désigner le web criminel au sens large, indépendamment de son indexation ou de son accessibilité. Dans l'imaginaire collectif, le *darkweb* regroupe donc ces deux définitions, c'est-à-dire à la fois les sites dédiés aux activités criminelles et les sites utilisant le réseau Tor, qu'ils soient dédiés au cybercrime ou non.

Deepweb

Le *deepweb*, ou « web profond », parfois même « web invisible », est souvent défini comme le web accessible mais non indexé par les moteurs de recherche. L'exemple le plus simple est celui d'un site web bancaire. Ce dernier possède une partie publique, référencée par les moteurs de recherche, et une privée, qui concerne les informations bancaires du client et se situe derrière un mécanisme d'authentification. La deuxième est accessible au client mais pas au moteur de recherche.

*

Les cybermenaces sont des tentatives malveillantes destinées à perturber un système informatique ou un réseau en volant des données ou en accédant à des fichiers non autorisés. Les cybermenaces touchent aussi bien les particuliers que les entreprises. Elles peuvent être une source de chantage (*ransomware*), de monétisation (revente d'infos personnelles sur le *darkweb*), ou d'usurpation d'identité (*phishing*, etc.).

---

[86] https://orangecyberdefense.com/fr/insights/blog/fuite_de_donnees/deepweb-darkweb-darknet-quelles-differences/
[87] Source : https://www.eset.com/fr/cybermenaces/

Ransomware

Ce type de logiciel est conçu pour verrouiller l'accès à un appareil ou en crypter le contenu, dans le but de vous extorquer de l'argent. Mais évidemment, vous n'avez aucune garantie que votre contenu ou votre appareil sera « libéré » après avoir payé. Découvrez comment vous protéger dans notre article.

Usurpation d'identité

L'une des principales motivations des personnes qui collectent frauduleusement vos données personnelles est d'utiliser ces données afin de se faire passer pour vous. C'est un crime grave qui peut parfois avoir de lourdes conséquences pour les victimes.

Cheval de Troie

Ce terme générique désigne tout logiciel malveillant qui cache son véritable but pour vous inciter à l'installer sur votre appareil. Techniques d'ingénierie sociale, exploitation de vulnérabilités, faux liens de téléchargement... Tout est bon pour endormir votre méfiance et infiltrer votre ordinateur.

Spam

Très répandu depuis bien longtemps (le premier spam connu date de 1978), le spam est un message, un e-mail ou tout type de message numérique que vous n'avez pas sollicité. Souvent irritant et ennuyeux et parfois dangereux, il faut savoir s'en prémunir

Phishing

Le *phishing*, ou hameçonnage, est une technique consistant à se faire passer pour une personne ou une entité en qui vous avez toute confiance, afin de vous soutirer des informations sensibles ou personnelles. Cela prend le plus souvent la forme d'un e-mail de votre banque semblant parfaitement authentique.

Spearphishing

Le *spearphishing* ou hameçonnage ciblé est une méthode de piratage qui, selon la définition de l'ANSSI « repose généralement sur une usurpation de l'identité de l'expéditeur, et procède par ingénierie sociale forte afin de lier l'objet du courriel et le corps du message à l'activité de la personne ou de l'organisation ciblée ».
Contrairement aux classiques tentatives d'hameçonnage (ou *phishing*)**,** le pirate tente de se faire passer pour une personne, une société ou un établissement avec lequel vous avez l'habitude de travailler pour vous faire baisser votre garde et vous pousser à ouvrir une pièce jointe corrompue ou un lien vers un site web malveillant.

Cryptojacking

Le domaine des crypto monnaies est assez récent, mais il n'a pas fallu longtemps pour qu'il attire des personnes mal intentionnées. Le but de ce procédé est d'utiliser, sans votre consentement, la puissance inutilisée de votre ordinateur pour extraire de la cryptomonnaie plus rapidement.

Malware

Malware (mot-valise pour « *malicious software* ») est un terme générique qui désigne tout type de logiciel malveillant. S'il est de plus en plus difficile de les identifier, leur point commun reste le même : un créateur de malware a forcément de mauvaises intentions.

Spywares

Un *spyware*, ou logiciel-espion, est un logiciel indésirable qui enregistre votre activité sur votre ordinateur, dans le but de collecter vos informations personnelles et vos habitudes de navigation, à l'abri des regards et surtout du vôtre.

Adwares

Les *adwares* sont des logiciels destinés à vous imposer des publicités, ce qui peut gêner voire empêcher votre navigation sur Internet. Ils peuvent aussi ralentir de manière durable le fonctionnement de votre ordinateur, ou bien servir à propager virus et autres spywares.

Rootkit

Le *rootkit* désigne un ensemble de logiciels destinés à prendre le contrôle de votre ordinateur, tout en restant le plus discret possible. Cette discrétion les rend extrêmement difficiles à identifier, d'autant que leurs opérations sont souvent invisibles pour l'utilisateur.

Faille Zero-Day

On appelle « faille *zero-day* » toute faille de sécurité dans un logiciel, une application ou un système informatique qui a été détectée mais pas nécessairement exposée, et surtout pour laquelle aucune solution de protection n'a encore été trouvée. Ces failles *zero-day* sont des brèches exploitables par les *hackers*, mais aussi et surtout un moyen pour eux de gagner de l'argent.

Annexe n° 4. Les principales cyber-attaques au plan international

Estonie (2007)

Le pays est victimes de plusieurs attaques par déni de service (Ddos) destinées à bloquer des sites gouvernementaux et bancaires ; ces attaques font suite au projet de déplacement de la statue d'un soldat soviétique.

Géorgie (2008)

De nombreuses attaques par déni de service (Ddos) précédent de 48 heures l'entrée en Ossétie du sud des troupes russes, provoquant le défaçage de nombreux sites gouvernementaux, affichant, par exemple, un photo montage montrant le président Saakachvili à côté d'Adolph Hitler.

Stuxnet (2010)

un virus informatique très probablement développé par les services de renseignement d'Israël et des États-Unis infecte le réseau de centrifugeuses iranien, destiné à enrichir l'uranium en vue de produire une arme nucléaire.

Dark Séoul (2013)

Plusieurs cyber-attaques, attribuées à la Corée du nord, frappent la Corée du sud en gelant les réseaux de trois chaînes de télévision et de plusieurs banques et institutions financières, en défaçant ou perturbant par déni de service (Ddos) plusieurs sites officiels et en publiant (« leaks ») les données personnelles de 2,5 millions de membres du parti de la Liberté et de militaires coréens et américains.

Sony Pictures (2014)

Le réseau du studio de cinéma est piraté suite au projet de sortie du film parodique *The interview* mettant en cause la Corée du nord ; cinq films, dont quatre devaient sortir en salles, sont publiées sur des plateformes de téléchargement.

TV5 Monde (2015)

Une attaque en défaçage affiche le drapeau de l'Etat islamique (DAESH) et se réclame du « cybercaliphate » sur le site de la chaîne et sur les réseaux sociaux, dont le réseau interne et la diffusion télévisuelle ont été compromis. Bien qu'affichant des slogans islamistes, cette attaque est généralement attribuée à un groupes para-étatique russe (APT28).

NotPetya (2017)

Un rançongiciel, ciblant initialement l'Ukraine, infecte plusieurs milliers d'ordinateurs dans le monde, et quelques centaines d'ordinateurs de la société Saint-Gobain, détruisant de nombreuses données.

SolarWinds (2020)

Le piratage du dispositif de mise à jour du logiciel Orion de la société SolarWinds a entraîné l'infection de plusieurs milliers d'ordinateurs du gouvernement américain et de grandes organisations publiques et privées américaines ; cette attaque sophistiquée par la chaîne d'approvisionnement (*supply chain attack*) est attribuée au service de renseignement russe SVR par l'intermédiaire de groupes para-étatiques[88].

Colonial pipeline (2021)

Un rançongiciel bloque le principal oléoduc de la côte ouest des États-Unis d'Amérique pendant plusieurs jours, menaçant l'approvisionnement en carburant jusqu'au paiement de la rançon.

Microsoft Exchange (2021)

Une faille de sécurité inconnue (*zero-day exploit*) permet à des pirates de s'introduire dans les serveurs de messagerie de nombreuses organisations aux États-Unis.

[88] Deux groupes sont plus particulièrement ciblés, selon le sobriquet qui leur est attribué par la communauté de cyberdéfense américaine, *Fancy Bear* (APT28) et *Cozy Bear* (APT29).

Annexe n° 5. L'activité du GIP

L'activité du GIP ACYMA en cinq opérations clés

(Source : rapport d'activité 2020 du GIP ACYMA)

1. Lancement de la plateforme *Cybermalveillance.gouv.fr*

Inauguré en 2017, le site assiste les victimes d'actes de cybermalveillance en proposant des conseils et/ou une mise en relation avec un professionnel en sécurité numérique de proximité susceptible de les assister techniquement. La plateforme propose également des contenus de prévention et de sensibilisation à la sécurité numérique. Deux années d'expérience qui ont permis une refonte du site en 2020 afin, notamment, de consolider les parcours victimes et d'ajuster au mieux les nouvelles modalités de mise en relation avec les professionnels en sécurité numérique.

2. Publication d'un kit de sensibilisation

Fruit d'une collaboration entre une vingtaine de membres du GIP ACYMA, cet outil vise à sensibiliser les publics en leur partageant les bonnes pratiques en matière de sécurité numérique, que ce soit dans leurs usages professionnels ou personnels. En cas de cyberattaque, le kit permet également aux internautes de comprendre les faits dont ils ont été victimes afin de les assister au mieux et faciliter d'éventuelles démarches administratives. Un an après la sortie du 1er volet en 2018, le kit de sensibilisation fut enrichi avec cinq nouveaux thèmes (réseaux sociaux, mots de passe, mises à jour…) et quatre nouveaux formats (quizz, bande-dessinée, poster…), dans un graphisme totalement repensé et des contenus accessibles à tous.

3. Diffusion de campagnes TV

Réalisation de campagnes d'information en partenariat avec l'Institut National de la Consommation et avec France Télévision. À destination des chaînes du groupe France Télévision, TNT, web TV et sites web, ces émissions et spots vidéo abordent des thématiques telles que les réseaux sociaux, les applications mobiles ou les achats en ligne.

4. Lancement de l'observatoire de la cybermalveillance

Grâce à la remontée des données d'utilisation des victimes par nos prestataires et leur qualification par nos experts, nous avons pu initier le lancement de l'observatoire du risque numérique en 2019. Réalisé en collaboration avec certains de nos membres, ce groupe de travail a pour objectif d'établir à l'échelle nationale des observations sur la cybermalveillance.

5. Mise en place du label ExpertCyber

Dans une démarche d'amélioration globale du niveau des professionnels en sécurité numérique, nous avons développé – en partenariat avec les principaux syndicats professionnels du secteur et le soutien de l'AFNOR – un label de qualité sur l'expertise numérique. Il s'agit d'un label qui atteste d'un certain niveau de compétences techniques, de bonnes pratiques et de transparence dans l'accompagnement des victimes.

Les partenariats spécifiques

(Source : rapport d'activité 2019 et 2020 du GIP ACYMA)

Avec la police judiciaire

Le début d'année 2019 voit l'amplification des campagnes de « crypto-porno » (chantage à la webcam prétendue piratée) et, par conséquent, du nombre de victimes. Ce phénomène est rapidement identifié par les magistrats spécialisés du pôle cybercriminalité, qui rédigent aussitôt un modèle de lettre plainte en collaboration avec la SDLC.

Cybermalveillance.gouv.fr a mis à disposition le document sur sa plateforme, permettant aux victimes de **formaliser leur plainte** et de partager des données techniques avec les enquêteurs. 28 000 concitoyens transmettent alors les éléments sur 140 000 visiteurs de la page dédiée. Grâce aux informations collectées, les services d'enquête identifient deux personnes. Elles sont interpellées en septembre, puis en décembre 2019.

Avec Pôle emploi

En collaboration avec Pôle emploi, *Cybermalveillance.gouv.fr* a produit trois nouvelles fiches pour adopter les bons réflexes face aux principaux types d'arnaque à l'emploi pouvant être rencontrés par les particuliers, les entreprises et les recruteurs.

Également intégrées dans les parcours de prévention et d'assistance aux victimes de la plateforme *www.cybermalveillance.gouv.fr*, ces fiches concernent les propositions d'emploi frauduleuses que peuvent recevoir des particuliers, les fausses offres d'emploi sur Internet et le piratage de l'espace personnel d'un recruteur sur un site d'emploi. Ces contenus sont relayés sur le site Internet et les différents supports de Pôle emploi, et mis à disposition des 34 600 conseillers.

Avec la FEVAD

Tous les deux ans, la Fevad publie avec l'INC un guide pratique pour accompagner les consommateurs lors de leurs achats en ligne. *Achats en ligne, Suivez le Guide* répond aux questions que peuvent se poser les cyberacheteurs avant, pendant ou après leurs achats sur internet.

Avec *Cybermalveillance.gouv.fr*, la Fevad et l'INC mettent également en garde dans ce guide contre l'hameçonnage ou *phishing*, une technique utilisée par le fraudeur pour obtenir les données personnelles des particuliers.

Annexe n° 6. La cybersécurité dans les entreprises

LE 6e BAROMÈTRE DE LA CYBERSÉCURITÉ DES ENTREPRISES[89] (FÉVRIER 2021) DU CLUB DE SÉCURITÉ DE L'INFORMATION FRANÇAIS

Une vulnérabilité des entreprises aux cyber-attaques toujours avérée.

57 % des entreprises déclarent avoir connu au moins une cyber-attaque en 2020 : une vulnérabilité toujours présente donc, malgré un taux en légère baisse par rapport à l'année dernière (65 %).

Une entreprise sur 5 (19 %) a été victime d'une attaque de type rançongiciels provoquant un chiffrement ou un volet chantage de données. Les entreprises, conscientes de la recrudescence de la menace rançongiciels en 2020 renforcent la sensibilisation des utilisateurs (83 %) à ce type d'attaque. Les vecteurs d'attaque par *phishing* (80 %) et exploitation des failles (52 %) restent les plus répandues, menant le plus souvent à un vol de données (30 %) ou à un déni de service (29 %). Une des principales causes de cyber-risques est le *ShadowIT*[90] pour 44 % des entreprises, suivies par la vulnérabilité résiduelle permanente (36 %) et la cyber-attaque opportuniste (36 %). Plus de la moitié des entreprises (56 %) estiment que le niveau des menaces relatives au cyber-espionnage est élevé. Similairement à l'année dernière, 58 % des cyber-attaques ont un impact sur le business, entraînant le plus souvent une perturbation de la production (27 %).

Les entreprises ne peuvent que progresser sur leur capacité à répondre aux attaques.

85 % des entreprises jugent les solutions de protection disponibles sur le marché plutôt adaptées aux besoins de leur entreprise. Elles sont d'ailleurs 69 % à s'estimer prêtes à gérer une cyber-attaque en termes de moyens de prévention, mais moins nombreuses à l'être en termes de moyens de détection (59 %). Pour ce faire, elles mettent en place en moyenne 10 solutions, et en priorité le VPN, le proxy & filtrage d'URL et la passerelle de sécurité mail. Toujours dans une démarche de prévention, 29 % des entreprises ont mis en place le concept de *ZeroTrust* et 45% sont en train de l'étudier. Toutefois, seules 46% des entreprises se disent confiantes quant à leur capacité de réponse à une cyber-attaque. 33 % des entreprises mettent en place un programme d'entraînement à la cyber-crise et 24 % ont déjà fait appel à leur cyber-assurance en cas d'attaque. 47 % des entreprises ont porté plainte à la suite d'une ou plusieurs cyber-attaques, mais seulement 15 % des enquêtes ont débouchés sur une identification ou une interpellation des attaquants.

La crise sanitaire apporte de nouveaux risques avec la généralisation du télétravail (37 %) et l'augmentation des crises cyber liée aux nouveaux risques (35 %). Par ailleurs, 43 % des entreprises se disent prêtes à augmenter les budgets liés à la cybersécurité pour faire face à ces nouveaux risques.

---

[89] *Source : CESIN, février 2021.*

[90] Le *Shadow IT* est l'utilisation de technologies matérielles et logicielles par les employés d'une entreprise sans l'accord du département informatique.

Une sensibilisation des salariés en continu.

77 % des entreprises estiment que leurs salariés sont sensibilisés à la cybersécurité, mais tous ne semblent pas appliquer les recommandations (63 %). D'après les responsables de la sécurité des systèmes d'information (RSSI), les usages numériques des salariés présentent de nombreux risques, et plus particulièrement l'utilisation de services cloud non approuvés (84 %) ou encore la gestion des partages de données à l'initiative des salariés (80 %).

Les RSSI mettent en avant plusieurs **risques à l'utilisation du Cloud**, les plus forts étant la non-maîtrise de la chaîne de sous-traitance de l'hébergeur (51 %), la difficulté de contrôler les accès par des administrateurs de l'hébergeur (45 %) et la non-maîtrise de l'utilisation qui en est faite par les salariés de l'entreprise (44 %). 86 % des entreprises estiment par ailleurs que les outils fournis par les prestataires de solutions Cloud ne permettent pas de sécuriser les données et qu'il est nécessaire d'utiliser des dispositifs et outils spécifiques.

Les entreprises sont **inquiètes, mais clairvoyantes** sur les enjeux de demain. Au final, une sur deux est inquiète quant à sa capacité à faire face aux cyber-risques. Les entreprises **identifient trois principaux enjeux pour demain :**

- placer la cybersécurité au centre de la gouvernance de l'entreprise (60 %), les entreprises se disent d'ailleurs confiantes quant à la prise en compte des enjeux de la cybersécurité au sein du COMEX (72 %/+8 points par rapport à 2019) ;
- former et sensibiliser les usagers à la cybersécurité (56 %), il s'agit d'un processus déjà mis en place puisque la sensibilisation est le premier dispositif (83 %) à avoir été renforcé par les RSSI face à la vague des cyber-attaques ;
- allouer davantage de budgets et de ressources à la cybersécurité (46 %). 57 %des entreprises comptent augmenter les budgets pour la protection contre les cyber-risques. En termes de ressources, les entreprises souhaitent augmenter les effectifs de cybersécurité (52 %). L'augmentation du budget passe également par l'acquisition de nouvelles solutions techniques désirée par 85 % des entreprises.

(…)

Annexe n° 7. Bilan et compte de résultat (2017-2020)

Bilan

	2 017	2 018	2 019	2 020
Immobilisations incorporelles	1 566	30 969	266 131	232 461
Immobilisations corporelles	10 776	26 034	40 862	47 775
Immobilisations financières				
TOTAL I	12 342	57 003	306 993	280 236
Avances et acomptes versés sur commandes		6 655		
créances clients et comptes rattachés		31 632		68 270
valeurs mobilières de placement				
Disponibilités	272 185,00	523 890	448 591	496 717
charge constatée d'avance	10 904	15 555	20 819	22 949
TOTAL II	283 089	577 732	469 410	587 936
TOTAL ACTIF	**295 431**	**634 735**	**776 403**	**868 172**
Fonds propres				
Financement de l'actif par l'Etat	14 793	11 982	9 171	9 171
Report à nouveau		258 499	598 637	587 344
Résultat	258 499,00	340 138	< 11 293 >	11 085
Total I	273 292	610 619	596 515	607 600
Provisions pour risques				
provision pour charges				
Total II				
Emprunt auprès établissement de crédit				
Dettes fournisseurs	10 849	26 980	186 224	78 178
Dettes fiscales et sociales	11 290,00	< 2 864 >	< 6 336 >	7 394
Dettes sur immobilisations et comptes rattachés				
Produits constatés d'avance				175 000
TOTAL III	22 139	24 116	179 888	260 572
TOTAL PASSIF	**295 431**	**634 735**	**776 403**	**868 172**

Source : Cour des comptes, d'après les comptes annuels déposés par le GIP Acyma

Compte de résultat

	2 017	2 018	2 019	2 020
PRODUITS				
Produits de fonctionnement				
Subventions de fonctionnement en provenance de l'Etat et des autres entités publiques	326 800	761 488	661 510	694 500
Autres subventions de fonctionnement		405 000	515 000	705 000
Dons et legs			15 000	
Autres produits de gestion			1,44	2
reprise sur amortissement, dépréciation et provision	106,51		799,62	295,97
reprise du financement rattaché à un actif		2 811,19	2 811,19	
Total produits de fonctionnement	**326 906,51**	**1 169 299,19**	**1 195 122,25**	**1 399 797,52**
Total des produits financiers		-	-	-
Résultat de l'activité (Perte)			11 292,69	
TOTAL DES PRODUITS	**326 906,51**	**1 169 299,19**	**1 206 414,94**	**1 399 797,52**
CHARGES				
Charges de fonctionnement				
Consommation de marchandises et approvisionnement, réalisation de travaux	31 455	404 878,50	620 584,83	625 542
Salaires et traitements	25 780,80	286 738,39	391 580,14	472 634,04
Charges sociales	7 666,58	94 371,37	131 641,36	159 785,86
Autres charges de personnel	280,86	4 890,00	5 283,00	7 560
Impôts, taxes et versements assimilés	3 118,02	34 461,41	49 365,83	54 920,31
Dotations aux amortissements	107	3 821,00	7 959,78	68 270,48
Total charges de fonctionnement	**68 407,67**	**829 160,67**	**1 206 414,94**	**1 388 712,65**
Total charges d'intervention		-	-	-
Total charges financières		-	-	0,02
Résultat de l'activité (bénéfice)	258 498,84	340 138,52		11 084,85
TOTAL DES CHARGES	**326 906,51**	**1 169 299,19**	**1 206 414,94**	**1 399 797,52**

Source : Cour des comptes, d'après les comptes annuels déposés par le GIP Acyma

Annexe n° 8. Fonds de roulement et besoin en fonds de roulement (2017-2020)

	2017	2018	2019	2020
Financement Etat /actif	14 793	11 982	9 171	9 171
report à nouveau		258 499	598 637	587 345
résultat	258 499	340 138	- 11 292	11 085
Capitaux propres	273 292	610 619	596 516	607 601
Total Dettes (emprunt + provisions pr risques et charges) (+)				
Total immobilisations (-) nettes	12 342	57 003	306 993	280 236
Fonds de roulement FR	**260 950**	**553 616**	**289 523**	**327 365**
Actifs circulants d'exploitation (stocks + clients) (+)		38 287		68 270
charges constatées d'avance (-)	10 904	15 555	20 819	22 949
Dettes d'exploitation (fournisseurs)	10 849	26 980	186 224	78 178
Dettes fiscales et sociales	11 290	-2 864	-6 336	7 394
Produits constatées d'avance				175 000
Autres dettes				
besoin en fonds de roulement BFR	**-11 235**	**29 726**	**-159 069**	**-169 353**
Trésorerie nette (FR-BFR)	**272 185**	**523 890**	**448 592**	**496 718**

Source : Cour des comptes, d'après les comptes annuels déposés par le GIP Acyma