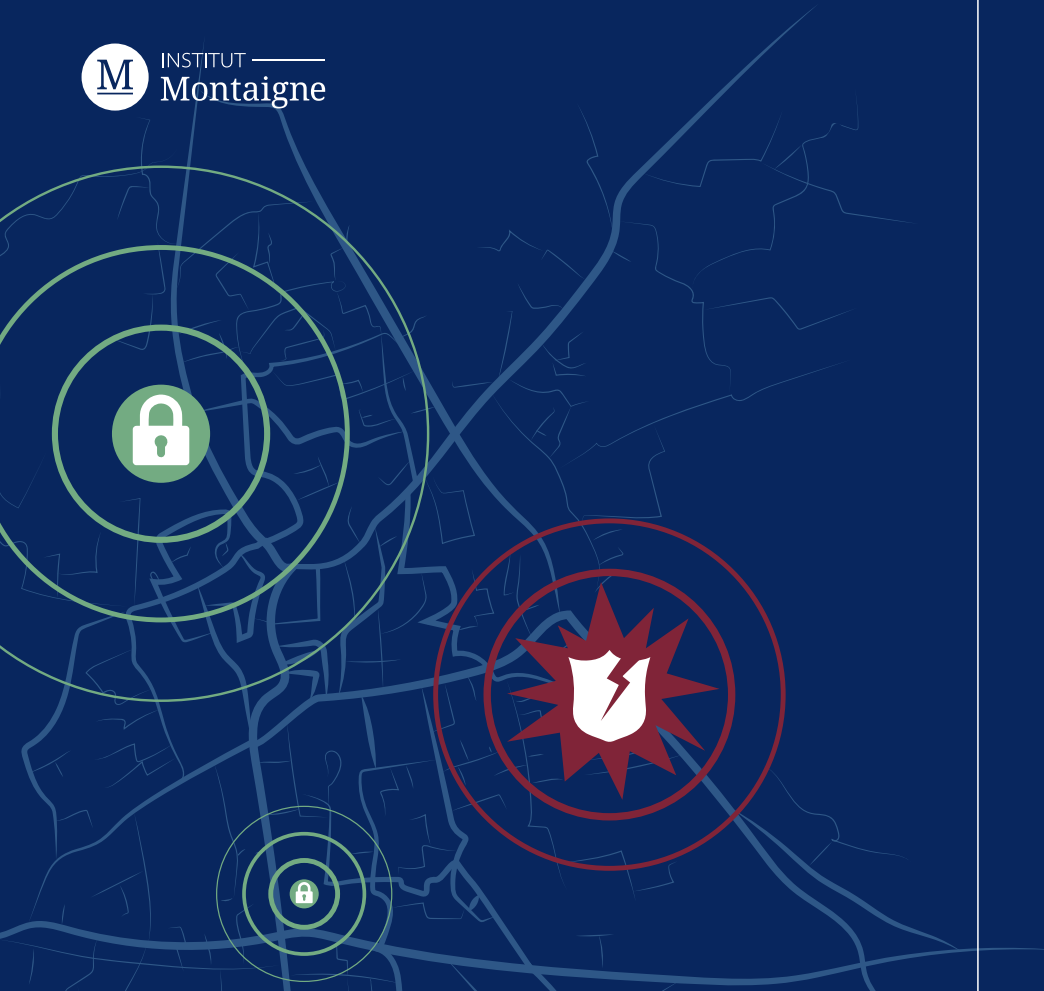
INSTITUT Montaigne



Cybersécurité

Passons à l'échelle

JUIN 2023

Think tank de référence en France et en Europe, l'Institut Montaigne est un espace de réflexion indépendant au service de l'intérêt général. Ses travaux prennent en compte les grands déterminants sociétaux, technologiques, environnementaux et géopolitiques afin de proposer des études et des débats sur les politiques publiques françaises et européennes. Il se situe à la confluence de la réflexion et de l'action, des idées et de la décision.

RAPPORT - Juin 2023

Cybersécurité

Passons à l'échelle

Les rapports de l'Institut Montaigne proposent des analyses exhaustives, issues d'une réflexion collégiale et ont vocation à identifier des solutions de long terme.

Table des matières

Synthèse

Historiquement, la cybersécurité a été d'abord une préoccupation des grandes entreprises à portée internationale, inquiètes de la protection de leurs flux de données et de leurs secrets industriels ou commerciaux. Sensibles au contexte mondial dans lequel elles évoluaient, elles ont été les premières à prendre des mesures pour se prémunir contre les cyberattaques. Aussi, les politiques régaliennes de sécurisation cyber se sont-elles essentiellement concentrées sur ces grands acteurs économiques et sur les entités critiques, laissant les plus petites structures - TPE/PME/ETI, collectivités et établissements de santé - très largement démunies et exposées aux dangers.

Deux éléments appellent aujourd'hui une correction rapide de ce désintérêt. Le premier est **l'intensification des menaces dans le cyberespace découlant de la mondialisation de la cybercriminalité.** L'élargissement de la surface d'attaque devient un facteur de déstabilisation économique et sociale potentiellement grave, qu'il s'agisse de bloquer l'activité d'une entreprise, d'un établissement de santé ou d'une collectivité, mettant en péril leur capacités opérationnelles, leur santé financière voire leur survie. Selon les chiffres gouvernementaux**, une PME sur deux fait faillite dans les 18 mois suivant une cyberattaque.** On estime également qu'**1 collectivité sur 10 (majoritairement de moins de 5000 habitants) a déjà été victime d'un rançongiciel.** Le coût, à lui seul, des attaques par rançongiciel subis pour les PME de moins de 50 employés est estimé à plus de 720 M€ par an.

Le second élément invitant à une action rapide est **l'application française de la directive européenne NIS 2 d'ici à septembre 2024**, dont les nouvelles orientations visent à entamer la diffusion de la cybersécurité dans l'ensemble de la chaîne numérique, précisément dans cette logique de sécurisation des maillons faibles. Une amende proportionnelle au chiffre d'affaires sera exigée en cas de non conformité. Surtout, ce respect de la directive sera une condition d'insertion des petits dans les chaînes de décision ou de valeur des plus grands.

Les entretiens menés pour cette étude révèlent tout à la fois **une prise de conscience de la menace cyber de la majorité des acteurs et une forte vo-**

lonté de passer à l'action, mais aussi un manque de moyens et d'accompagnement pour franchir le pas. Peu d'entreprises rendent compte des attaques subies. Une minorité des acteurs locaux (principalement des petites communes et de très petites entreprises) reste néanmoins soit inconsciente des risques, soit rétive à la prise en compte de la menace car ne se sentant pas concernée.

En effet, les entités de taille modérée font rarement de la cybersécurité une priorité, et lorsqu'elles s'y intéressent, le manque de visibilité de ce qu'elles doivent faire, le manque de compétences disponibles, le manque de financement et l'existence d'une multitude de solutions techniques contribuent à les décourager d'agir. Pourtant, la littérature facilement accessible recèle d'excellentes recommandations pour tout responsable cherchant à mieux protéger sa structure. Encore faut-il savoir par où commencer et vers qui se tourner, comment anticiper les risques et comment réagir en cas d'attaque.

Des mesures spécifiques adaptées à ces acteurs doivent donc être proposées. Côté pouvoirs publics, beaucoup d'excellentes choses existent déjà et les acteurs de l'État sont unanimement reconnus pour leur professionnalisme et leurs compétences. Mais la répartition de leurs prérogatives n'est pas nécessairement maîtrisée et le besoin de moyens additionnels ne croît pas au rythme de la menace. Surtout, la coordination de leurs actions est un impératif aux échelles appropriées des structures à protéger – régions, départements, communes. Et cette coordination doit non seulement s'appliquer à prévenir les cyberattaques, elle doit aussi traiter au mieux leur remédiation et leur répression.

Ainsi, il apparaît nécessaire de **créer les conditions d'un passage à l'échelle pour mobiliser à tous les niveaux et protéger plus exhaustivement le territoire.** Cependant, ce nécessaire passage à l'échelle de la part des acteurs locaux publics et économiques est confronté à deux impératifs contradictoires. Face à l'urgence de la situation, le premier plaide pour des mesures d'obligation afin d'accélérer le pas. Au vu du besoin de pédagogie et d'accompagnement d'acteurs qui se sentent démunis, le second plaide pour une approche moins rigide, centrée sur l'incitation.

Le rapport propose ainsi une **approche incrémentale**.

- Dans un premier temps, il a semblé nécessaire de se concentrer sur ce que les entreprises et collectivités pouvaient faire par elles-mêmes et de les accompagner au plus près dans cette montée en sensibilisation et en protection autonome.

- Dans un deuxième temps, la contrainte réglementaire poussera naturellement ces acteurs à une prise en charge minimale des enjeux de cybersécurité.

- Enfin, une approche plus contraignante pourra être envisagée auprès des plus rétifs afin d'élargir la couverture territoriale et d'assurer un niveau minimum de cybersécurité à l'échelle du pays.

Dans cette démarche de rehaussement collectif du niveau de cybersécurité, l'Institut Montaigne a proposé **une méthode simple et rapidement opérationnelle fondée sur les solutions et acteurs existants.**

À cette fin, à partir du constat partagé, de **nombreux entretiens ont été conduits avec des personnages-clé de l'écosystème français de la cybersécurité.** Pour les compléter, des experts de ce même écosystème et des entreprises adhérentes à l'Institut Montaigne se sont réunis et ont collaboré pour imaginer et consolider les réponses adaptées.

Plus spécifiquement, **une dizaine d'ateliers thématiques ont été conduits** réunissant entreprises, experts et acteurs de terrain, en partenariat avec le Mouvement des entreprises de taille intermédiaire (METI) et la Gendarmerie nationale. Cette approche collaborative a permis un constat partagé de la situation et l'identification des pistes les plus utiles pour mieux sensibiliser responsables et employés des structures visées. Les ateliers se sont appliqués à identifier les types de produits de sécurité numérique les plus adaptés – dans une logique du juste besoin, et les modalités d'accompagnement des bénéficiaires. La question de la maîtrise des risques et du modèle assurantiel possible a été sérieusement examinée, tandis que le sujet des financements et de la nécessaire mutualisation des solutions ont fait l'objet d'une attention

particulière. Enfin, les enjeux de simplification du signalement, de remédiation et d'action judiciaire ont été intégrés à la réflexion.

Ces ateliers ont ensuite été complétés par des **études de terrain**, auprès d'entreprises nationales et locales, de collectivités territoriales et d'un Centre Régional de Réponse à Incidents (CSIRT). Ces études ont permis de **tester la validité des recommandations** au plus près des acteurs engagés sur le terrain.

Le coût annuel global de cet effort de passage à l'échelle pour les petites entreprises et collectivités représenterait une centaine de millions d'euros, englobant tant les moyens humains nécessaires que les subventions en faveur d'offres mutualisées et des structures qui les portent.

Axe 1 :

Mobiliser les acteurs locaux en faveur d'un parcours de cybersécurité simple et progressif à même de les protéger et de les préparer aux crises : diagnostic, ambition, précautions, exercices et organisation

RECOMMANDATION 1 : Inciter à recourir à des diagnostics organisationnels et techniques en proposant un référentiel commun comprenant différentes profondeurs de diagnostic

RECOMMANDATION 2 : Fixer une cible de cybersécurité à atteindre pour les structures, en fonction de leur criticité et de leurs moyens, et les inciter à progresser dans la durée en proposant un système de badges les aidant à prioriser leurs arbitrages

RECOMMANDATION 3 : Limiter nativement la présence de vulnérabilités et de failles dans les poduits et équipements numériques disponibles sur le marché européen en exploitant tout le potentiel du règlement européen *Cyber Resilience Act*, et informer les utilisateurs en temps réel en cas de trafic Internet suspect grâce à une "cyber vigie" opérée par les opérateurs de télécommunications

RECOMMANDATION 4 : Exhorter les entreprises et collectivités à considérer le risque cyber comme une préoccupation stratégique encadrant les choix humains, organisationnels, budgétaires et techniques de leur activité

RECOMMANDATION 5 : Organiser une simulation annuelle d'alerte cyber (équivalent de "l'alerte incendie") pour tous les salariés ou agents d'une entreprise ou d'une collectivité, afin de les acculturer à la menace et aux bonnes pratiques numériques

RECOMMANDATION 6 : Instaurer une fonction de conseiller à la sécurité numérique (CSN) auprès de chaque responsable de structure (dirigeant d'entreprise ou élu) pour accompagner celui-ci sur les questions de cybersécurité

Axe 2 :

Coordonner les ressources, les outils et les prérogatives de chaque acteur aux échelles appropriées : nouveaux moyens nationaux et mutualisations locales

RECOMMANDATION 7 : Mutualiser les compétences et les outils chez les acteurs de confiance publics et privés en charge de la cybersécurité afin de permettre une couverture complète du maillage territorial

RECOMMANDATION 8 : Faciliter le signalement des attaques cyber via une "Plateforme de Signalement des faits Cyber", base de données commune aux différents services publics compétents en matière de cybersécurité, permettant un suivi consolidé

RECOMMANDATION 9 : Renforcer les moyens et l'organisation des acteurs de la lutte contre la cybercriminalité dans une logique de proximité, en mettant l'accent sur la prévention et sur la répression

RECOMMANDATION 10 : Pérenniser le financement de l'effort public en faveur d'une sécurité numérique collective par un abondement vertueux des budgets

Cette étude à la fois globale et territoriale a montré l'urgence d'une action coordonnée aux différentes échelles du territoire. L'expérience de terrain invite à un pragmatisme volontaire qui mobilise chaque acteur de la sécurité numérique à son juste niveau.

Au niveau national, l'ANSSI porte l'ambition de la sécurité numérique nationale et promeut les solutions et outils les plus pertinents pour les acteurs concernés. Les services de l'Intérieur portent les enjeux de prévention et d'investigation, couplés avec la Justice pour la partie sanctions.

Au niveau local, les conseils régionaux, les préfectures, la gendarmerie et la police nationales, et autres services de l'État, les chambres consulaires et les collectivités ont tous un rôle à jouer de sensibilisation, de formation, d'anticipation des attaques et de collecte d'informations. Le secteur privé a essentiellement une responsabilité d'accompagnement, d'ingénierie technique et de remédiation en cas de problème.

Les conditions clés pour un passage à l'échelle effectif et réussi reposent essentiellement sur l'articulation des efforts de ces différents acteurs en temps réel et la mobilisation rapide des moyens identifiés.

Côté entreprises et petites collectivités, la priorité est à la compréhension des enjeux, l'acceptation des accompagnements disponibles et la mise en place des outils proposés (diagnostic et mise à niveau personnalisée).

La conviction des professionnels du secteur est qu'il suffit parfois de peu pour améliorer la sécurité des structures, pour autant que celles-ci en comprennent l'utilité et en acceptent les modalités pratiques. Le numérique irriguant désormais tous nos usages, la sécurité doit devenir un réflexe naturel, comme le port de la ceinture de sécurité dans les voitures ou la fermeture de la porte d'entrée de sa maison : un comportement de bon sens que personne ne remet en cause.

Introduction

Si la cybersécurité est souvent considérée comme une problématique purement technique, celle-ci recouvre en réalité une multitude d'enjeux cruciaux tels que la compétence des professionnels de la sécurité, les enjeux budgétaires, sociaux, humains et organisationnels. Ces facteurs sont tout aussi importants que les briques techniques pour garantir une protection efficace contre les cyberattaques. Pour permettre une prise en compte globale de la cybersécurité et un passage à l'échelle pour une protection accrue, dans un contexte de hausse croissante de la menace cyber, il est primordial de réfléchir aux moyens et leviers permettant d'étendre le cercle de protection cyber des grandes entreprises stratégiques jusqu'aux plus petites entreprises et collectivités.

La cybersécurité, en tant que "*état d'un système numérique garantissant la résistance à des événements, issus du cyberespace, susceptibles d'affecter la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ce système offre ou qu'il rend accessibles*"[1,2] est un enjeu majeur pour toutes les entreprises et collectivités, qu'elles soient grandes ou petites. En raison de la numérisation croissante des activités et l'émergence toujours plus aiguë des nouvelles technologies dans les usages courants, entreprises et administrations sont devenues de plus en plus exposées aux menaces cyber.

Face à cet accroissement de la menace cyber, en particulier d'origine criminelle mais aussi étatique, certains pays, dont la France, ont mis en œuvre une politique de sécurisation cyber visant prioritairement les acteurs les plus importants - grandes entreprises et entités régaliennes critiques - et d'amorcer la sensibilisation des petites et moyennes entités telles que les TPE/PME/ETI, les petites collectivités et la plupart des établissements de santé.

Dès lors, ces entités les moins préparées se retrouvent aujourd'hui particulièrement exposées à la menace cyber. Pourtant, selon une enquête IFOP[3] , seu-

[1] https://hal-mines-paristech.archives-ouvertes.fr/hal-01781568/document
[2] https://www.ssi.gouv.fr/entreprise/glossaire/c/
[3] https://www.ifop.com/publication/les-pme-et-la-cybersecurite/

lement 11 % des PME françaises déclarent avoir déjà été la cible d'une cyberattaque. Ce résultat, bien qu'important, est très probablement sous-évalué en raison du coût réputationnel pour une entreprise de faire savoir qu'elle a été victime de cyberattaque, ou simplement parce qu'une partie significative des PME peut ne pas identifier avoir subi une cyberattaque (un vol de données, par exemple).

Ce manque de prise de conscience des risques cyber par les petits acteurs n'est pas sans soulever un risque systémique. En effet, comme illustré par les différents exemples listés ci-dessous, la réalisation simultanée de la menace cyber sur une multitude de TPE/PME/ETI, de petites collectivités ou d'hôpitaux peut induire une véritable disruption de la vie économique et sociale :

- pour une collectivité territoriale, le blocage du système d'information par une cyberattaque peut empêcher le bon versement aux administrés des prestations sociales essentielles (revenu de solidarité active, allocation personnalisée d'autonomie, etc.), comme en témoigne le chiffrement récent (mai 2023) par un rançongiciel de la Collectivité territoriale de Martinique[4] ;

- pour un hôpital, une cyberattaque peut perturber grandement les opérations médicales en bloquant le processus d'admission des patients, voire en rendant inaccessibles les machines indispensables pour établir des diagnostics ;

- pour une TPE/PME/ETI, une cyberattaque peut mettre hors d'usage des processus clés de l'entreprise tels son système de production (outils de commande-machine), son système de prise de commande ou de facturation, son système d'ERP, empêchant ainsi son activité, ses prises de commandes ou ses ordres de livraison et entraînant possiblement une paralysie de toutes ses activités opérationnelles. Un tel blocage est susceptible de mettre en péril sa santé financière et conduire potentiellement à sa faillite : selon une déclaration du ministre délégué chargé de la Transition numérique, **une PME sur deux fait faillite dans les 18 mois suivant une cyberattaque[6] .**

[4] *https://www.martinique.franceantilles.fr/actualite/societe/un-gang-de-hackeurs-aurait-revendique-la-cyberattaque-de-la-ctm-939078.php*

[5] *Un ERP (Enterprise Resource Planning) est un système informatique intégré qui permet à une entreprise de gérer et d'automatiser ses processus commerciaux, opérationnels et financiers à l'aide d'une base de données centralisée.*

Une cyberattaque est un événement marquant pour l'ensemble des employés, déroutant pour la direction et les responsables informatiques qui sont soumis à un stress intense pendant la durée de la crise. Les données de la structure, parfois définitivement perdues, parfois vendues, peuvent entraîner la dissolution (pour une entreprise), et des conséquences juridiques et financières très importantes.

Dans ce contexte d'une menace généralisée où toute structure peut être victime, le présent rapport vise, d'une part, à faire un état des lieux de la menace cyber et des dispositifs déjà en place pour y faire face et, d'autre part, à sensibiliser sur le caractère systémique des questions de sécurité numérique et à encourager l'adoption de mesures spécifiques et adaptées s'adressant à l'ensemble des acteurs, en particulier pour les acteurs les moins matures sur ce thème - TPE/PME/ETI, petites collectivités locales et hôpitaux, de manière à asseoir l'émergence d'un véritable "passage à l'échelle" de la cybersécurité en France.

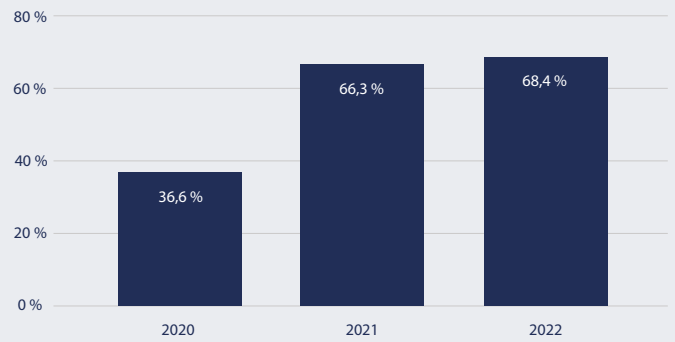
[6] *https://rendre-notre-monde-plus-sur.goron.fr/bpifrance-a-la-rescousse-des-pme-avec-diag-cybersecurite/*

1 Les quinze dernières années ont été marquées par une intensification des cyberattaques qui a particulièrement affecté les TPE/PME/ETI et les collectivités locales

1. LA TRANSFORMATION NUMÉRIQUE A ACCRU L'EXPOSITION DE L'ÉCONOMIE ET DE LA SOCIÉTÉ À DES MENACES CYBER QUI ONT EXPLOSÉ AU COURS DES 5 DERNIÈRES ANNÉES

Les technologies numériques se sont rapidement diffusées dans l'ensemble de notre société et ont transformé les modalités d'interaction entre individus et de transmission de l'information, tant dans la sphère publique que privée. Ainsi, selon le baromètre France Num de 2022, 68 % des entreprises françaises disposaient d'un site Internet présentant leur activité, contre 37 % en 2020.

Site internet présentant l'activité de l'entreprise (hors réseaux sociaux) : taux d'équipement



Source : baromètre France Num de 2022[7]

[7] https://data.economie.gouv.fr/pages/barometre-france-num/liens-jdd#echantillons-des-enqutes

Si ces technologies offrent de nombreuses opportunités, **leur utilisation accrue induit une exposition croissante à des menaces cyber de plus en plus sophistiquées, voire destructrices.**

L'attaque informatique attribuée par l'OTAN[8] à la Fédération de Russie ayant ciblé l'Estonie en 2007, ainsi que la diffusion massive du rançongiciel[9] Wannacry[10] en mai 2017 - infectant plus de 300 000 ordinateurs dans plus de 150 pays - suivie de celle du *wiper* NotPetya en juin 2017[11] ayant bloqué environ 2000 entreprises (dont Saint-Gobain pour un coût estimé de 220M€), ont marqué deux séquences dans l'accélération mondiale du phénomène ces 15 dernières années.

Le groupement d'intérêt public (GIP) ACYMA observe sur sa plateforme Cybermalveillance.gouv.fr, dont la mission est de sensibiliser et d'assister les particuliers, les associations, les collectivités et les entreprises face aux cyberattaques, une hausse constante des demandes d'assistance depuis sa création en 2017 avec 280 000 demandes d'assistance en 2022 contre environ 30000 en 2018, soit une hausse moyenne d'environ 75 % par an[12] .

[7] *https://data.economie.gouv.fr/pages/barometre-france-num/liens-jdd#echantillons-des-enqutes*

[8] *https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf*

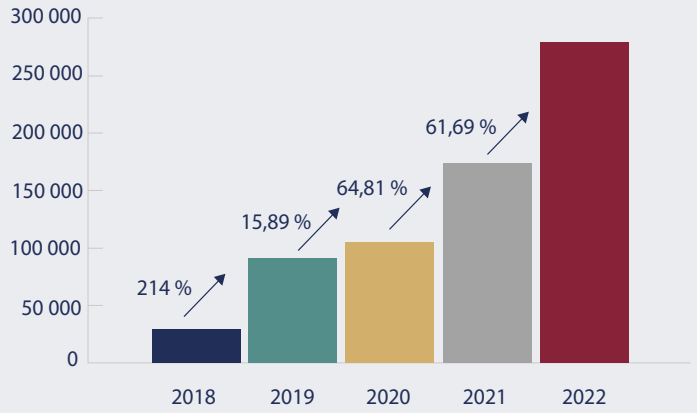
[9] *Un rançongiciel (ransomware en anglais) est un code malveillant visant à chiffrer les données du système d'information de la victime où il est déployé. Les attaquants contactent ensuite celle-ci pour lui demander une rançon en échange de la clé de déchiffrement.*

[10] *https://fr.wikipedia.org/wiki/WannaCry*

[11] *https://www.hiscox.fr/sites/france/files/documents/cp-2017-cyber-top-10-cyberattaques.pdf*

[12] *Ces chiffres souffrent de plusieurs biais. D'une part, les demandes d'assistances sous-évaluent très certainement le nombre total d'attaques cyber, les victimes déposant peu plainte (1 fois sur 250 environ), et signalant peu d'éventuelles pertes de données personnelles (même lorsqu'elles en ont l'obligation). D'autre part, il est plausible que le nombre de demandes d'assistance augmente en partie parce que la plateforme Cybermalveillance.gouv.fr, créée en 2017, est de plus en plus connue. En outre, les sollicitations sur le site peuvent sortir du cadre strict des cyberattaques. Néanmoins d'autres chiffres corroborent cette hausse importante : selon l'entreprise AV Test, spécialisée dans la cybersécurité, le nombre de cyberattaques impliquant le recours à un maliciel (malware) a crû de 37 % par an en moyenne entre 2011 et 2020.*

Nombre de demandes d'assistance en ligne
sur la plateforme *Cybermalveillance.gouv.fr*



Source : Cybermalveillance.gouv.fr, Rapport d'activité 2022[13]

Cette augmentation de la consultation, en particulier liée au développement de la notoriété du site, reflète également une hausse du nombre de cyberattaques. Elle peut s'expliquer, d'une part, par la structuration et l'organisation d'un écosystème cybercriminel qui se professionnalise, liées à la diffusion d'un arsenal numérique toujours plus vaste (place de marchés pour le *trading* de vulnérabilités, réutilisation de code d'exploitation qui ont fuité, etc.) ; et, d'autre part, par une généralisation des usages numériques dont le fonctionnement des infrastructures sous-jacentes est souvent mal maîtrisé par une majorité des particuliers, des entreprises et des administrations, augmentant de fait les surfaces d'attaque susceptibles d'être exploitées par des acteurs malveillants[14] .

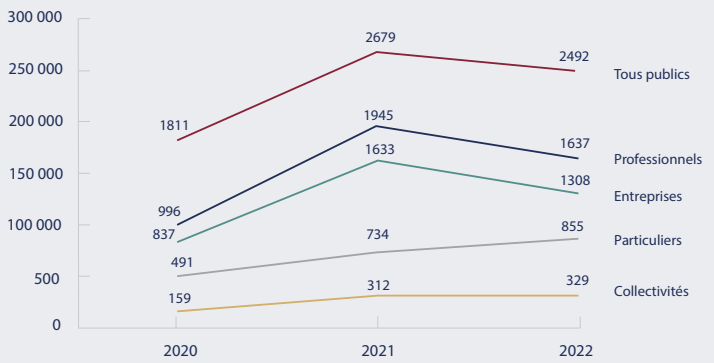
[13] https://medias.vie-publique.fr/data_storage_s3/rapport/pdf/288757.pdf
[14] *Panoramas 2021 et 2022 de la menace (Agence nationale de la sécurité des systèmes d'information)*

I.2. LA MULTIPLICATION DU NOMBRE D'ATTAQUES INFORMATIQUES DÉCOULE PRINCIPALEMENT DE LA STRUCTURATION DE L'ACTIVITÉ CYBERCRIMINELLE, CAUSE ET CONSÉQUENCE D'UN FORT DÉVELOPPEMENT DES RANÇONGICIELS

Parmi les cyberattaques, les attaques par rançongiciel, logiciel malveillant pour chiffrer les fichiers d'un système informatique et demander une rançon en échange de leur déchiffrement, ont connu un essor important sur les 5 dernières années. Celles-ci seraient devenues à la fois plus nombreuses et plus rentables.

Premièrement, en termes de volume, la plateforme Cybermalveillance.gouv.fr a observé une forte hausse des recherches d'assistance sur les attaques par rançongiciel entre 2020 et 2021 (avec une multiplication par un facteur 2 pour les entreprises et les collectivités), suivie d'une légère baisse en 2022.

Évolution du nombre de recherches d'assistance
sur les attaques par rançongiciel

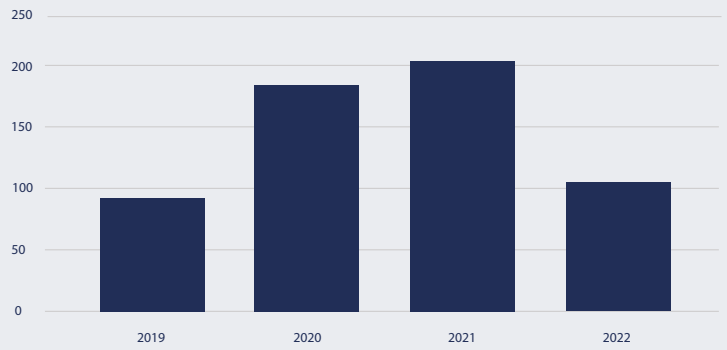


Source : Cybermalveillance.gouv.fr, Rapport d'activité 2022[15]

[15] https://medias.vie-publique.fr/data_storage_s3/rapport/pdf/288757.pdf

De son côté, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a pu observer, entre 2019 et 2021, une très forte hausse du nombre d'attaques par rançongiciels qui lui ont été signalées, suivie d'une forte baisse[16] en 2022 (-50 % par rapport à 2021).

Évolution du nombre d'attaques par rançongiciels signées à l'ANSSI entre 2019 et 2022



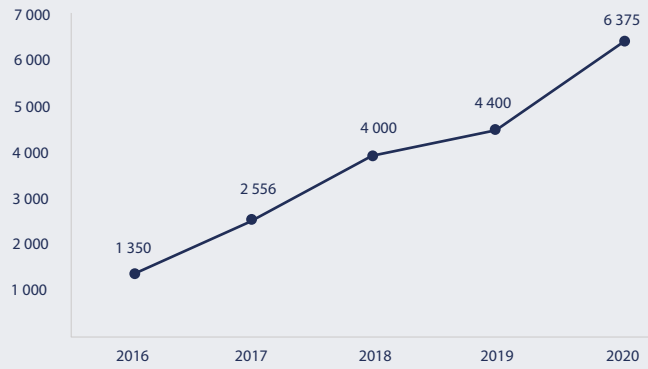
Source : ANSSI, Panoramas de la menace 2021[17] et 2022[18]

Cette baisse récente peut s'expliquer par le fait que les grandes structures, souvent soumises à des obligations réglementaires (de signalement des cyberattaques à l'ANSSI, notamment), sont désormais bien mieux protégées face aux attaques par rançongiciel. Cette baisse pourrait aussi s'expliquer par le fait que les plus petites entités non régulées (TPE, PME et certaines ETI) font plus souvent le choix de recourir directement à un prestataire privé pour la réponse à incident, sans prévenir l'ANSSI ni même Cybermalveillance.gouv.fr. Pour cette raison, le phénomène observé ne constitue ainsi que la partie immergée de l'iceberg et le nombre total d'attaques reste impossible à déterminer. Ainsi, l'infiltration et la saisie des serveurs hébergeant le service de

[17] https://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_panorama-menace-ANSSI.pdf
[18] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf

rançongiciel Hive, en janvier 2023 par un consortium international (incluant, entre autres, le FBI et Europol), a permis de découvrir qu'**environ 80 % des 1300 victimes du rançongiciel (entre juin 2021 et novembre 2022) ne s'étaient jamais signalées auprès des autorités[19].** Dès lors, il convient de garder à l'esprit que les chiffres fournis par Cybermalveillance.gouv.fr et l'ANSSI sont, très certainement, fortement sous-estimés. En effet, en s'appuyant sur une étude d'Emsisoft (cf. annexe 3), on peut estimer plusieurs dizaines de milliers de compromissions par rançongiciels environ en France chaque année, toutes entités publiques ou privées confondues (hors particulier)[20] .

Évolution de la valeur médiane du montant des rançons en France de 2016 à 2020 (en euros)



Source : Service Statistique Ministériel de la Sécurité intérieure, bases des victimes et délits enregistrés par la police et la gendarmerie entre 2016 et 2020[21]

[19] https://apnews.com/article/technology-politics-health-crime-us-department-of-justice-ed17a8853d78a9d0185af04cb8bd2fd2
[20] *Emsisoft obtient le chiffre de 18 000 compromissions par rançongiciel en France en multipliant par quatre les 4476 soumissions sur la plateforme "ID Ransomware" et en faisant l'hypothèse que seulement 25 % des victimes utilisent cette plateforme d'identification de souches de rançongiciel. En formulant une hypothèse plus réaliste de 10 % de recours à la plateforme d'identification des souches, le chiffre serait de 45 000 compromissions par rançongiciels environ en France pour l'ensemble des secteurs public et privé.*
[21] https://www.interieur.gouv.fr/content/download/129878/1034435/file/IA37.pdf

Deuxièmement, en termes de rentabilité, la valeur médiane du montant des rançons est en constante augmentation de 2016 à 2020, selon des statistiques issues du ministère de l'Intérieur.

Le montant de la rançon dépend généralement du type de victime :

- quelques milliers d'euros pour un particulier ;
- entre quelques milliers et plusieurs centaines de milliers d'euros pour les TPE/PME ;
- entre quelques centaines de milliers à plusieurs centaines de millions d'euros pour les ETI et grandes entreprises.

S'agissant du montant moyen, une comparaison internationale d'Emsisoft évoque un montant d'environ 33 000 € (pour chaque rançon demandée en France en 2020, à des entités publiques comme privées - le montant évolue entre chaque pays de 10 % environ, cf. annexe 3).

Cet essor des attaques par rançongiciel, en termes de volume et de rentabilité, peut s'expliquer par plusieurs facteurs :

- **L'apparition des crypto-monnaies**[22] a largement facilité le processus de blanchiment de l'argent issu du paiement de la rançon.
- Lors d'attaques cyber, **L'augmentation importante des gains financiers acquis par les acteurs cybercriminels en quelques années a entraîné une professionnalisation de ces derniers**, elle-même accélérant le développement des rançongiciels au travers d'un cercle vicieux. Grâce à des gains financiers annuels estimés par l'ANSSI à environ 1 Md€ en 2021 pour les seuls revenus de rançongiciels, de nombreux types de rançongiciels ont dès lors émergé : en 2021, l'ANSSI suivait en moyenne une quarantaine de souches différentes de rançongiciels[23] (souvent issues de la sphère russophone avec des groupes tels que Lockbit ou anciennement Conti) tandis que plus d'une trentaine de souches ont été identifiées au sein des procédures judiciaires enregistrées par la Gendarmerie au cours de l'année 2021.
- **Lors d'attaques cyber, les données obtenues sont régulièrement exfiltrées avant leur chiffrement par un rançongiciel, pour être mises en vente ou être mises à disposition ("leakées") gratuitement en cas de non-paiement de la rançon (double extorsion).** Dès lors, ces données, susceptibles de contenir des noms d'utilisateur, des mots de passe ou d'autres types d'identifiants, peuvent être utilisées par d'autres groupes cybercriminels pour mener des campagnes d'hameçonnage crédibles visant à rançonner d'autres entreprises[24].

La professionnalisation des acteurs cybercriminels s'est accompagnée d'une spécialisation autour d'une myriade de métiers qui correspondent aux différentes étapes d'une attaque informatique :

- **fournisseurs de codes malveillants** (avec les opérateurs de rançongiciels qui vendent ou louent leur code selon le modèle du "*ransomware-as-a-service*", ou encore les places de marché proposant des codes permettant d'exploiter des vulnérabilités) ;
- **services d'hébergement sans aucun contrôle** tels que les "*bullet proof hosters*"[25] (dont les infrastructures sont souvent hébergées dans des juridictions hors d'atteinte des traités de coopération judiciaire) ;
- **vente d'accès initiaux à des réseaux compromis** ("*access brokers*" proposant à la vente, par exemple, toutes sortes d'identifiants de connexion dérobés) ;

[22] *Le bitcoin, mais aussi bien d'autres, généralement moins traçables par nature ou par l'utilisation de mixers. https://www.avanista.fr/actualites/59-rancongiciels-quel-role-joue-la-cryptomonnaie*

[23] *https://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_panorama-menace-ANSSI.pdf*

[24] *https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf*

[25] *Les "bullet-proof hosters" offrent des services d'hébergement (serveurs dédiés, noms de domaine et autres infrastructures réseau) à des individus ou des organisations qui cherchent à mener des activités illicites en ligne, telles que le phishing, la distribution de logiciels malveillants, le piratage, la diffusion de contenus illégaux, etc. Ils peuvent également fournir des services tels que la protection contre les attaques DDoS (Distributed Denial of Service) pour aider à maintenir en ligne les sites web liés à ces activités illégales.*

- **services d'envoi de pourriels** (*spam*), notamment pour faire du hameçonnage ciblé ;
- **plateformes de "mixage" de crypto-monnaies** pour blanchir les rançons.

Dans ce contexte de professionnalisation des cybercriminels qui ont l'embarras du choix de potentielles victimes, en particulier grâce aux opportunités d'exploitation à large échelle offertes par la vente massive d'accès initiaux, les attaques par rançongiciels réussies se concentrent sur les entités les plus faiblement protégées ; **autrement dit, les hyènes se rabattent sur les gazelles les plus lentes du troupeau.** Outre la vente massive d'accès, la grande majorité de cybercriminels peuvent attaquer en masse, du fait des possibilités offertes par les outils numériques et la structuration des réseaux. Donc, à mesure que des acteurs (grandes entreprises, États) montent en compétence défensive, les autres subissent, par report, la majorité des attaques. Certaines vulnérabilités sont toujours exploitées, alors qu'elles sont anciennes et souvent corrigées de longue date par les éditeurs.

En outre, certaines attaques, simples ou complexes, peuvent être conduites par des Etats (directement ou indirectement via des groupes constitués). Les finalités de ces attaques sont souvent différentes des finalités criminelles, puisqu'il s'agira de déstabiliser, d'espionner, de saboter, notamment. Ces ingérences sont contrées par des parades spécifiques conduites par des services de l'Etat. Néanmoins, tous les acteurs, même les entreprises ou collectivités, peuvent être visés. Améliorer sa cybersécurité pour éviter une menace criminelle permet du même coup de limiter une partie des risques numériques provenant d'une menace étatique.

I.3 FACE À CETTE INTENSIFICATION DES CYBERATTAQUES, LES SECTEURS RÉGALIENS ET STRATÉGIQUES ONT PU BÉNÉFICIER D'UNE SÉCURISATION PROGRESSIVE, QUE CE SOIT À L'ÉCHELLE NATIONALE OU EUROPÉENNE

Face à l'intensification de la menace cyber, les autorités françaises et européennes ont mis en oeuvre une logique de sécurisation cyber par cercles concentriques, en soumettant dans un premier temps seuls les acteurs les

plus importants et les plus critiques à des obligations réglementaires strictes, puis en élargissant progressivement l'assiette d'acteurs concernés.

En France, le concept d'opérateurs d'importance vitale (OIV)[26], instauré en 2006, a été complété d'un volet de sécurité informatique par la loi de programmation militaire (LPM) de 2014-2019. Les OIV correspondent aujourd'hui à environ 250 opérateurs[27] publics ou privés[28], notamment dans les secteurs bancaires, des transports, de l'alimentation, des télécommunications, de la défense ou de l'énergie, dont les activités sont indispensables au bon fonctionnement et à la survie de la Nation.

[26] Les secteurs d'activité d'importance vitale (SAIV) englobent des opérateurs d'importance vitale (OIV).
[27] https://www.sgdsn.gouv.fr/publications/la-securite-des-activites-dimportance-vitale
[28] Leur liste est classifiée pour des raisons de sécurité nationale.

La loi de programmation militaire (LPM) 2014-2019 et les livres blancs sur la sécurité nationale

Les premières législations ayant trait aux questions de sécurité numérique[29], intervenues très tôt, ont été tenues à jour et sophistiquées à de multiples reprises pour trouver à s'appliquer sans discontinuité, de sorte que certains ont pu évoquer une inflation normative. La loi informatique et liberté, par exemple, a été amendée à 41 reprises depuis 1978.

Les livres blancs sur la sécurité nationale (2008, 2013) ont permis la création de l'ANSSI, mettant notamment l'effort sur la sécurisation des activités critiques, la diffusion de bonnes

[29] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique

pratiques de sécurité numérique, et l'émergence d'une filière française de cybersécurité pour développer des produits de confiance.

La LPM impose à ces OIV, d'une part de renforcer la sécurité des systèmes d'information critiques qu'ils exploitent (les "systèmes d'information d'importance vitale", ou SIIV) et, d'autre part, de signaler à l'ANSSI tout soupçon d'intrusion sur ces derniers.

Face à l'augmentation en quantité et en sophistication des attaques informatiques, c'est l'ANSSI qui a pour mission de les accompagner dans la sécurisation de leurs SIIV.

La France est le premier pays de l'Union européenne à avoir adopté un dispositif législatif visant à assurer la cybersécurité de ses infrastructures critiques.

Le livre blanc sur la sécurité intérieure (2020) a renforcé le caractère prégnant de la menace et la nécessité de renforcer la réponse de l'État, en s'appuyant sur les forces de sécurité, leur maillage territorial et leurs unités d'investigation numérique.

Un texte à venir : la LPM 2024-2030

La loi de programmation militaire 2024-2030, en cours de discussion au Parlement, vise à introduire de nouvelles dispositions en matière de cybersécurité et tend à renforcer les prérogatives de l'ANSSI pour lui permettre d'assurer sa mission de défense des infrastructures critiques de la Nation.

L'une des dispositions phares de cette loi est la possibilité pour l'ANSSI de bloquer les noms de domaine utilisés par les pirates informatiques, avec un contrôle a posteriori de l'Autorité de régulation des communications électroniques (ARCEP), afin de permettre à l'ANSSI de réagir plus rapidement et plus efficacement en cas d'attaque informatique systémique affectant concomitamment un grand nombre d'entités sur le territoire.

Le projet de loi prévoit également de nouvelles obligations de signalement pour les éditeurs de logiciels touchés par une cyberattaque ou ayant découvert une vulnérabilité critique sur un produit utilisé en France. Cette mesure concorde en partie avec le projet de règlement européen *Cyber Resilience Act* portée par la Commission européenne (cf. infra).

En outre, la LPM entend étendre les dispositifs de détection des cyberattaques fonctionnant sur l'analyse des flux réseau, en renforçant les possibilités déjà offertes par les articles 34-1 et 34-2 de la LPM 2019-2025. Ces articles permettent déjà à l'ANSSI de rechercher des marqueurs techniques dans les logs des opérateurs de télécommunications (article 34-1) et d'installer des sondes réseau derrière des serveurs hébergés en France suspectés de mener des activités malveillantes (article 34-2).

Enfin, le projet de loi vise à obliger les fournisseurs d'accès à internet (FAI), sur demande de l'ANSSI, à communiquer certaines données techniques relatives au cache de leurs serveurs DNS pour permettre à l'ANSSI connaître les requêtes DNS anonymisées effectuées par les clients, qu'ils soient légitimes ou malveillants, afin de suivre l'infrastructure mise en place par un attaquant.

En Europe, la directive NIS 1 (voir encadré ci-dessous), inspirée de l'approche française (portée par la LPM 2014-2019) et adoptée en juillet 2018, a introduit les opérateurs de services essentiels (OSE) qui doivent respecter des exigences fortes en matière de cybersécurité. En France, environ 300 entités sont concernées.

Néanmoins, le réexamen de la directive NIS 1 a révélé des hétérogénéités dans sa mise en œuvre par les États membres, en particulier en ce qui concerne son champ d'application qui a largement été laissé à la discrétion des États membres.

Dans ce contexte, la directive NIS 2, publiée le 27 décembre 2022, vise à harmoniser et étendre ces exigences en matière de cybersécurité à un nombre encore plus important de secteurs d'activité sensibles, publics et privés, pour les entités comptant plus de 50 personnes. En France, environ 7000 à 15000 entités seront concernées.

Les directives européennes NIS 1 et NIS 2

LA DIRECTIVE NIS 1

Dans le contexte de l'accélération de la transformation numérique des sociétés européennes et de l'interconnexion des États membres, la directive "Network and Information Security" (NIS), adoptée en juillet 2016 par le Parlement européen et le Conseil de l'Union européenne, visait à augmenter collectivement le niveau de sécurité face aux cybermenaces auxquelles était exposé le marché européen.

Transposée au niveau national en 2018, cette directive oblige

chaque État membre à renforcer la cybersécurité d'entités (dans 19 secteurs clés) nommées "opérateurs de services essentiels" (OSE), jugées indispensables au fonctionnement de l'économie et de la société.

Une fois désignées par les différents États membres, ces OSE sont dans l'obligation, d'une part, de prendre des mesures techniques et organisationnelles appropriées pour garantir un niveau élevé de sécurité de leurs réseaux et de leurs systèmes d'information (SI) et, d'autre part, de déclarer tout incident de sécurité ayant un impact significatif sur la continuité de leurs services essentiels à l'autorité nationale compétente.

Pour s'assurer de la bonne application de la directive NIS, chaque État membre doit désigner une ou plusieurs autorités nationales compétentes ayant notamment pour rôle de conseiller, et éventuellement d'assister, les OSE en matière de cybersécurité. En France, il s'agit de l'ANSSI[30] .

LA DIRECTIVE NIS 2

Pour faire face, d'une part, au morcellement du marché intérieur induit par des transpositions hétérogènes de la directive NIS 1 et, d'autre part, à un écosystème cyber-malveillant toujours plus développé et affectant un nombre croissant d'entités mal protégées, la directive NIS 2, adoptée en novembre 2022, élargit le périmètre d'application de la directive NIS 1 pouraccroître le niveau de cybersécurité au sein de l'Union.

[30] *https://www.ssi.gouv.fr/actualite/directive-nis-lanssi-accompagne-les-premiers-operateurs-de-services-essentiels/*

Transposée par une législation nationale d'ici septembre 2024, la directive NIS 2 élargira le périmètre des anciens OSE régulés (en opérant une distinction entre "**entités essentielles**" et "**entités importantes**"), à des milliers d'entités correspondant à 35 secteurs (administrations centrales et régionales, certaines collectivités territoriales, transports, secteur bancaire, infrastructures des marchés financiers, santé, eau, infrastructures numériques, la gestion des services TIC, espace, gestion des déchets, distributeurs alimentaires, etc.) et 600 types d'entités différentes : administrations de toutes tailles et des entreprises allant des PME (de plus 50 employés ou affichant un chiffre d'affaires ou un bilan supérieur à 10M€) aux groupes du CAC40. A cette occasion, le nombre d'entités entrant dans l'assiette de l'ANSSI sera, au minimum, multiplié par 10.

La directive NIS 2 incite également toutes les entités, qu'elles soient régulées ou non, à recourir à des outils de cybersécurité en sources ouvertes, en particulier les petites et moyennes entreprises souhaitant atteindre un bon niveau tout en limitant les coûts.

La directive NIS 2 mentionne également que "les États membres devraient disposer d'un point de contact pour les petites et moyennes entreprises au niveau national ou régional, qui [leur] fournisse soit des orientations et une assistance, soit les oriente vers les organismes appropriés pour leur fournir des orientations et une assistance en ce qui concerne les questions liées à la cybersécurité".

Concrètement, la directive NIS 2 s'appliquera, une fois transposée en droit interne, à un nombre d'entités qui reste à déterminer. De manière générale, cette dernière devrait globalement s'appliquer aux entreprises des secteurs concernés comptant plus de 50 salariés (grandes entreprises, ETI, PME) réalisant plus d'un million d'euros de chiffre d'affaires, ainsi qu'aux collectivités locales à partir d'une certaine taille.

Les TPE/PME de moins de 50 salariés (ou dont le chiffre d'affaires est inférieur à 10M€) et les petites collectivités locales devraient en rester exclues (ce point est laissé à l'appréciation de chaque État). En tout état de cause, la directive énonce que la charge ainsi imposée aux entités essentielles ou importantes devra être proportionnée aux risques encourus et à leurs capacités financières.

Quel que soit le niveau final retenu pour l'application de la directrice, la question de la capacité de passage à l'échelle se pose[31],considérant le niveau initial de maturité : les futures structures ciblées ont probablement un niveau de maturité en cybersécurité assez éloigné de ce qui leur sera demandé.

Un dernier aspect essentiel de la directive porte sur le durcissement de son système de sanctions en comparaison de la directive NIS 1. Le mécanisme envisagé, qui ressemble beaucoup à celui du RGPD (Règlement Général de Protection des Données), pourra déterminer les pénalités en fonction des infractions commises, en se basant sur un pourcentage du chiffre d'affaires mondial de l'entité impliquée, et non plus sur un montant forfaitaire.

[31] Pour les entités "importantes", la directive dispose par exemple que le niveau à atteindre doit être fonction de leurs moyens et de la menace.

I.4. CES ATTAQUES CYBER SE RABATTENT DÉSORMAIS DE FAÇON INDISCRIMINÉE SUR LES CIBLES LES PLUS ACCESSIBLES : EN FRANCE, LES TPE/PME/ETI, LES COLLECTIVITÉS ET LES ÉTABLISSEMENTS DE SANTÉ SONT PARTICULIÈREMENT AFFECTÉS

Les dispositifs législatifs et réglementaires adoptés ces dernières années, à l'échelle européenne comme nationale, ont permis aux grandes entreprises et aux entités critiques régaliennes d'atteindre un niveau de sécurisation suffisant pour se prémunir très largement des attaques informatiques conduites par les nouveaux modes opératoires des cybercriminels.

La conséquence de la sécurisation des plus grands acteurs est un déplacement du ciblage des cyberattaques vers les entités moins protégées, à l'instar des TPE/PME/ETI et des petites collectivités locales. Ainsi, la somme de ces structures (et établissements publics de santé) représente 73 % des attaques par rançongiciels portés à la connaissance de l'ANSSI en 2022 (contre 65 % en 2020); tandis que les entreprises stratégiques, correspondant pour la plupart à de grands groupes, ne représentent plus que 6 % des victimes de compromission par rançongiciels en 2022 (contre 24 % en 2020).

Répartition des types de victimes de compromission par rançongiciels en 2020, 2021 et 2022

Type de structure	2020	2021	2022
TPE/PME/ETI	34 %	51 %	40 %
Collectivité territoriale/locale	24 %	19 %	23 %
Entreprise stratégique	24 %	9 %	6 %
Établissement public de santé	7 %	7 %	10 %
Établissement d'enseignement supérieur	4 %	3 %	8 %
EPA, EPIC	3 %	3 %	4 %
Ministère	0 %	1 %	2 %
Autre (association, infrastructures de transport, etc.)	4 %	6 %	6 %
Total : petites et moyennes entreprises + collectivités + établissements publics de santé	65 %	77 %	73 %

Source : ANSSI, Panoramas de la menace 2021[32] et 2022[33]

Grâce à l'achat d'identifiants d'accès à des réseaux compromis obtenus préalablement par d'autres acteurs *via* des campagnes non ciblées et massives[34], **les groupes cybercriminels employant des rançongiciels compromettent généralement des entités manquant de protection numérique.** Si les cybercriminels visent a priori des entités dont ils pensent qu'ils pourront tirer un gain financier, ces attaques parfois indiscriminées touchent même des structures incapables de payer les rançons demandées. C'est par exemple

[32] https://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_panorama-menace-ANSSI.pdf
[33] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf
[34] *Ces identifiants d'accès sont vendues sur des places de marché nommées "access brokers" (cf. supra), à un prix qui dépend essentiellement de l'intérêt financier afférent à l'entité compromise*

le cas du Centre Hospitalier Sud Francilien, dont le SI a été chiffré par le rançongiciel Lockbit en août 2022, qui s'est vu demander une forte rançon.

Les vecteurs d'attaque généralement utilisés pour le déploiement d'un rançongiciel sont la compromission d'accès au protocole d'accès à distance (Remote Desktop Protocol ou RDP) et l'hameçonnage ciblé[35]; ces deux techniques d'intrusion initiale étant généralement suivies d'une latéralisation sur le réseau de la victime parl'intermédiaire de l'Active Directory[36].

S'il peut arriver que les attaquants aient une connaissance insuffisante de l'aisance financière de leur cible, ils réalisent parfois un travail préalable de renseignement et d'analyse[37].

D'ailleurs, les experts considèrent parfois que les attaquants de petit niveau s'attaquent aux cibles faciles (les plus nombreuses), et que les attaquants de haut niveau s'attaquent aux cibles très protégées (beaucoup moins nombreuses mais pour lesquelles le potentiel de gain est plus important) dans le cadre d'une pratique nommée *big game hunting*.

Néanmoins, l'accroissement du ciblage des TPE/PME/ETI et des petites collectivités par les modes opératoires cybercriminels n'induit pas que les grandes entreprises ou administrations sont complètement exemptes de risques face à ces menaces. En effet, un groupe cybercriminel qui compromet une petite entreprise, sous-traitante d'une grande entreprise, peut potentiellement exploiter, par opportunisme, une interconnexion existante entre les systèmes d'information pour se latéraliser vers la grande entreprise. C'est ce que l'on appelle une **attaque par chaîne d'approvisionnement.**

[35] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf

[36] *L'Active Directory est le service de gestion des utilisateurs, des ordinateurs et des ressources au sein d'un réseau informatique Windows.*

[37] *Notamment grâce aux techniques d'ingénierie sociale, parfois sur la seule base des informations disponibles en source ouverte.*

I.5. LES ENTITÉS LES MOINS PRÉPARÉES ET LES PLUS VULNÉRABLESSONT AUSSI LES PLUS NOMBREUSES, CE QUI N'EST PAS SANS INDUIRE UN RISQUE SYSTÉMIQUE TANT SUR LES PLANS FINANCIER, PSYCHOLOGIQUE OU ORGANISATIONNEL

I.5.a. Les collectivités

La France compte au total environ 45 000 collectivités locales[38] : environ 35 000 communes, 1 255 établissements publics de coopération intercommunale à fiscalité propre (métropoles, communautés urbaines, communautés d'agglomération, communautés de communes) et 8 882 établissements publics de coopération locale (syndicats sans fiscalité propre, de types SIVU, SIVOM, etc.), ainsi que les régions, les départements et les territoires d'outre-mer.

2⁄3 des Français vivent dans de petites collectivités locales, de densité intermédiaire à très peu denses. Les communes de moins de 3 500 habitants représentent 91 % des communes françaises (où habitent 31,4 % de la population). S'agissant de l'échelon intercommunal, 28 % des établissements publics de coopération intercommunale (EPCI) regroupent moins de 15 000 habitants et 35 % des EPCI regroupent entre 15 et 30 000 habitants. Seuls 10% des EPCI comptent plus de 100 000 habitants.

Schématiquement, plus les collectivités sont petites, moins elles sont conscientes, sensibilisées et préparées. D'après Data Publica pour la Banque des Territoires, 26 % des communes de moins de 3 500 habitants pensent ne pas être exposées au risque cyber, et le sujet de la cybersécurité n'est même pas pris en compte dans 34 % de ces communes. Seules 13 % des communes de moins de 3 500 habitants et 29 % de celles de 3 500 à 10 000 habitants ont désigné un responsable de la sécurité des systèmes d'information (RSSI), contre 71 % des communes de plus de 100 000 habitants. Seules

[38] https://www.collectivites-locales.gouv.fr/files/Accueil/DESL/WEB-Chiffres-cle%CC%81s%20des%20CL%202022.pdf

23 % des petites communes (< 3 500 habitants) ont déjà organisé des actions de formation, contre 80 % des régions et 57 % des communes de plus de 100 000 habitants.

Une collectivité sur dix a déjà été victime d'un rançongiciel selon les données de juin 2023 issues des diagnostics Di@GoNal (menés par la Gendarmerie auprès de 965 collectivités, dont 22 d'Outre-mer et 769 communes de moins de 5 000 habitants). De plus, 40 % n'avaient pas de délégué à la protection des données, **54 % ont déclaré ne pas avoir de référent cybersécurité** et **75 % n'étaient pas dotés d'un plan de gestion de crise cyber.**

Concernant les collectivités territoriales, les conséquences d'une compromission par rançongiciel ne sont pas seulement financières. En effet, ces attaques sont susceptibles de perturber des services tels que la paie[39], le versement des prestations sociales, la gestion de l'état civil, et d'une façon générale de nombreux services publics[40] essentiels à la vie de la cité. Le **risque de compromission des données à caractère personnel**, s'il n'est pas spécifique aux collectivités, revêt ici un caractère plus sensible (de nature matrimoniale, patrimoniale, fiscale, sociale...).

Depuis septembre 2022, l'ANSSI a d'ailleurs observé une forte augmentation des attaques par rançongiciels ciblant des collectivités territoriales[41].

I.5.b. Les TPE/PME/ETI

Environ **deux tiers des salariés** en France travaillent dans des TPE, PME ou ETI, qui elles-mêmes génèrent environ le tiers de la valeur économique annuelle du pays et les **deux tiers de la valeur économique produite par les entreprises.**

[39] Des salaires comme des factures de titulaires de marchés notamment
[40] Assurés en régie (par la collectivité elle-même) ou par délégation (par un prestataire).
[41] Avec notamment la ville de Caen (fin septembre 2022), le département de Seine-Maritime (en octobre 2022), le département de Seine-et-Marne (en novembre 2022) ou encore la région Normandie (en décembre 2022).

Catégorie d'entreprise	Effectif	Nombre d'employés (EQTP[42])	Valeur ajoutée HT	% valeur ajoutée (entreprises)	% valeur ajoutée (France)
Grandes entreprises (GE)	270	3,9 M	349 Mds€	31 %	18 %
ETI 250 à 4 999 salariés et CA < 1,5 Md€	5 841	3,4 M	284 Mds€	26 %	15 %
PME (hors TPE) 10 à 250 salariés et CA < 50M€	144 617	3,9 M	261 Mds€	23 %	13 %
TPE (micro-entreprise) <10 salariés et CA < 2M€	3 963 561[43]	2,2 M	218 Mds€	20 %	11 %
Total	4 114 289	13,4 M	1112 Mds€	100 %	57 %

Sources : Caractéristiques des entreprises par catégorie (INSEE, 2020)[44], Les entreprises en France (INSEE, 2020)[45]

Si les grandes entreprises ont désormais mis en œuvre des mesures pour assurer leur cybersécurité, **la grande majorité des entreprises - petites, moyennes et de taille intermédiaire - sont une cible du fait du manque de ressources consacrées à la cybersécurité** et de leur maîtrise limitée de cette thématique, parfois confiée à un prestataire externe (pour les entreprises les mieux préparées).

[42] Équivalent temps plein.
[43] Dont 3,2 millions d'entreprises unipersonnelles sans employés (soit environ 800 000 TPE comptant au moins un employé)
[44] https://www.insee.fr/fr/statistiques/2016091#tableau-figure1
[45] https://www.insee.fr/fr/statistiques/5758744?sommaire=5759063

En 2020, une **entreprise sur cinq déclare avoir subi au moins une attaque** par rançongiciel au cours de l'année et **58 % des cyberattaques ont eu des conséquences avérées** sur l'activité économique[46].

Les attaques peuvent engendrer des conséquences importantes sur les chaînes d'approvisionnement, via des blocages de l'appareil productif, des délais allongés, ou en perturbant les opérations des fournisseurs et des partenaires commerciaux :

- certaines entreprises ont mis la clé sous la porte après plus de 30 ans d'activité car leurs données clients ont été chiffrées[47];
- un fabricant de lingerie, avec plus de 1 000 salariés, s'est retrouvé en redressement judiciaire après que tous ses postes de travail aient été bloqués[48];
- un voyagiste a déploré[49] le vol de données courant mai 2023, portant sur les données d'au moins 10 000 passeports.

In fine, les répercussions peuvent engendrer des pertes financières à plusieurs niveaux, y compris auprès d'autres acteurs économiques qui ne sont pas directement victimes de la cyberattaque (et, souvent, ignorent que leurs données ont été compromises).

[46] https://www.senat.fr/rap/r20-678/r20-678_mono.html
[47] https://www.ipi-ecoles.com/impact-piratage-informatique-pme-pmi/
[48] https://www.oppens.fr/faillite-pme-cyberattaque-lise-charmel/
[49] https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/l-agence-voyageurs-du-monde-victime-d-une-cyberattaque-il s-font-les-malins-pour-pas-grand-chose-rassure-le-pdg-du-groupe_5871401.html

À cet égard, les ETI constituent une cible de choix étant donné que ces dernières génèrent 1000 Md€ de chiffre d'affaires et représentent 25 % de l'emploi en France en 2021, selon le METI[50].

Les coûts cumulés résultant des attaques par rançongiciel subis par l'ensemble des PME de moins de 50 employés en France sont estimés à environ 700M€ par an[51]. Si ce montant est éloigné de la valeur ajoutée générée par ces entreprises (de l'ordre de 650 Mds€/an), il est plus pertinent de considérer que ces coûts impactent directement l'investissement productif ou la trésorerie des entreprises.

L'effet d'une cyberattaque pour une ETI ou une petite/moyenne entreprise n'est pas seulement financier, mais également d'ordre psychologique et organisationnel. Ainsi, une étude de l'Université de Portsmouth[52],commanditée par leministère de l'Intérieur britannique, a révélé que les cyberattaques peuvent provoquer des séquelles psychologiques aussi graves que celles laissées par un cambriolage. En effet, de nombreux ressorts psychologiques sont mobilisés au cours de la chaîne d'infection sous-jacente à une cyberattaque.

Par exemple, en amont d'une attaque, le hameçonnage est une technique d'accès initial à un réseau informatique reposant sur la psychologie humaine, puisqu'elle implique de manipuler ou tromper la victime en l'incitant à ouvrir un lien ou une pièce jointe malveillante. Pour maximiser ses chances de succès, l'attaque cherche souvent en amont, dans le cadre d'une phase de reconnaissance, des informations personnelles sur les personnes composant l'entreprise cible, afin d'écrire le courriel le plus à même de correspondre à la vie quotidienne des collaborateurs.

Plus en aval, une fois qu'un rançongiciel a été déployé sur le réseau, une lutte psychologique s'engage entre l'attaquant et sa victime afin de persuader

[50] *Guide opérationnel à l'usage des Entreprises de Taille Intermédiaire, METI IDF, 2022*
[51] https://www.irt-systemx.fr/wp-content/uploads/2019/06/ISX-rancongiciels.pdf
[52] https://researchportal.port.ac.uk/en/publications/assessing-the-seriousness-of-cyber crime-the-case-of-computer-misu

celle-ci que le paiement de la rançon est le seul moyen pour celle-ci de récupérer ses données. Afin d'augmenter la pression, l'attaquant peut menacer la victime de ne jamais déchiffrer les données, mais également de diffuser tout ou partie de celles-ci sur Internet (double extorsion).

L'impact d'une cyberattaque peut également être d'ordre réputationnel. À cet égard, les cabinets d'avocats, qui sont parfois de petites structures dotées d'un SI peu protégé mais hébergeant souvent des données sensibles, sont tout particulièrement exposés. En effet, pour un cabinet, la divulgation de données personnelles à l'issue d'une cyberattaque peut violer le secret professionnel et engager la responsabilité des avocats en vertu de la loi Informatique et Libertés et du RGPD européen[53]. Par d'exemple, à la suite de la compromission d'un cabinet d'avocat français ayant représenté des parties au procès de l'attentat contre Charlie Hebdo, des éléments du dossier d'instruction ainsi que des données personnelles liées aux enquêteurs et magistrats suivant le dossier ont été publiées sur Internet[54].

I.5.c. Les établissements de santé

Les hôpitaux bénéficient depuis des années d'une attention particulière de l'ANSSI, en particulier les structures les plus importantes. Au-delà d'une attention de l'administration centrale de la santé, le niveau régional dispose de nombreux leviers[55], et semble un pivot dans la démarche.

Environ 900 établissements publics[56] sont regroupés en 135 groupements hospitaliers[57] de territoire (GHT), chargés de piloter la cybersécurité. Ceux-ci disposent des personnels formés et ont accès aux parcours de sécurité de

[53] http://www.audentia-gestion.fr/CNIL/CNIL-Guide_Avocats.pdf
[54] https://www.francetvinfo.fr/economie/medias/charlie-hebdo/info-franceinfo-attentat-contre-charlie-hebdo-un-cabinet-d-avocats-pirate- des-elements-du-dossier-publies-sur-internet_4856149.html
[55] *Via les Groupements régionaux d'appui au développement de la e-santé (GRADES), sous l'autorité des Agences régionales de santé (ARS).*
[56] https://esante.gouv.fr/sites/default/files/media_entity/documents/mss_ans_rapport_public_observatoire_signalements_issis_2021_vf.pdf
[57] https://www.reseau-hopital-ght.fr/actualites/sante-publique/politique-de-sante/350-millions-d-euros-pour-renforcer-la-cybersecurite-de s-etablissements-de-sante-et-medico-sociaux.html

l'ANSSI. Ils peuvent néanmoins avoir du mal à améliorer suffisamment leur cybersécurité, notamment pour des questions d'adhésion du personnel à ces nouvelles contraintes[58], de conduite du changement ou d'un manque de personnels formés. En raison du nombre d'attaques les touchant, de leur caractère critique et de leur aspect médiatique, des efforts récents et un plan dédié ont été mis en œuvre. Les quelques ensembles hospitaliers majeurs seraient des opérateurs d'importance vitale, tandis que la totalité des établissements chefs-lieux (support) de GHT seraient[59] des opérateurs de service essentiels. L'application de la directive NIS 2 devrait renforcer cette dynamique, en faisant de chaque hôpital un opérateur "important".

S'agissant de la question des établissements privés (cliniques, EHPAD...) leur situation paraît plus diverse. Il faut notamment distinguer les établissements médicaux, médico-sociaux et les professionnels de santé, dont les physionomies, états initiaux et besoins sont différents. Ils sont globalement à rapprocher des entreprises de tailles et chiffres d'affaires comparables.

S'agissant de la question des outils, le secteur présente la particularité d'être tourné vers des centrales d'achat.

Les personnels hospitaliers pourraient nécessiter une révolution culturelle en matière de cybersécurité ; certains redouteraient une complexification liée à une sécurisation accrue des usages numériques.

Les établissements de santé représentent néanmoins une cible facile[60],où se trouvent encore "des dizaines de milliers de postes fonctionnant sous Windows XP, des appareils médicaux achetés dans les années 90 ou 2000...". Ces systèmes sont donc moins protégés[61] , et plus facilement perméables aux nouvelles techniques d'attaque.

[58] *L'hygiène numérique représentant certaines contraintes supplémentaires, et la cybersécurité se présentant comme une priorité nécessaire mais qui apparaît moins critique que des investissements médicaux, par exemple.*
[59] *La divulgation précise est impossible, les informations détaillées devant rester confidentielles.*
[60] https://www.usine-digitale.fr/article/cyberattaques-contre-les-hopitaux-la-question-n-est-pas-de-savoir-si-cela-va-arriver-mais-quand.N2 092896
[61] *Les produits sont parfois isolés dans les systèmes d'information, mais la garantie n'est pas totale.*

Or, en cas de chiffrement du système d'information d'un hôpital par un rançongiciel, les conséquences peuvent être extrêmement graves. Si peu de données sont disponibles sur des décès directs ou indirects (en raison d'une inertie dans les soins qu'aurait provoquée l'attaque), ce sont généralement les systèmes supports qui sont visés et impliquent un déplacement de nombreux patients vers les établissements voisins afin de leur garantir un suivi optimal. La confidentialité des données de santé est susceptible d'être atteinte; de telles fuites de données entraînent une violation du RGPD exposant l'hôpital à une sanction administrative de la CNIL ainsi qu'à des actions juridiques en dommages et intérêts de la part des patients lésés.

Encore récemment, trois mois après la cyberattaque l'ayant touché en décembre 2022, un centre hospitalier des Yvelines n'a recouvré que 60 % de ses capacités opérationnelles[62]. Un centre hospitalier de l'Essonne, attaqué en août 2022, a dû envoyer, pour sa part, environ 1 million de courriels et de lettres à ses patients et ex-patients afin de les avertir de la potentielle fuite de leurs données personnelles médicales à la suite de la publication par le groupe cybercriminel Lockbit de l'ensemble des données exfiltrées lors de l'attaque[63].

I.5.d. La spécificité française ultra-marine

L'outre-mer (18 % du territoire terrestre, 4 % de la population française) représente une vulnérabilité spécifique. Dans de nombreux secteurs, et à plus forte raison dans celui de la santé, la résilience face à une cyberattaque est permise par la redondance. Concrètement, un hôpital ne pouvant plus fonctionner (pour cause de cyberattaque, par exemple), fait transporter ses patients vers les établissements hospitaliers environnants. Et l'on peut imaginer qu'il en va de même dans de nombreux secteurs : une entreprise voyant son exploitation limitée par une cyberattaque, voit son activité en partie reprise par ses concurrents.

[62] *https://www.capital.fr/economie-politique/lhopital-andre-mignot-de-versailles-bloque-depuis-trois-mois-par-une-cyberattaque-massive- 1464519*

[63] *https://www.francebleu.fr/infos/sante-sciences/cyberattaque-a-l-hopital-de-corbeil-essonnes-des-donnees-extremement-sensibles-divul guees-1664860289*

L'outre-mer pose la difficulté d'une bien moindre capacité de redondance; donc, d'une moindre résilience de ce point de vue, d'une plus grande dépendance que la métropole en cas de crise, et donc d'une plus grande sensibilité. En effet, les renforts et moyens supplémentaires, qu'il serait possible de dédier à un territoire touché spécifiquement, sont rares, et le temps de transport peut être important. **La cybersécurité des acteurs ultramarins pourrait donc devenir d'une certaine façon une priorité.**

I.6. DES INITIATIVES ONT ÉTÉ MISES EN PLACE DE FAÇON INCRÉMENTALE POUR ACCOMPAGNER LA CYBERSÉCURITÉ DES SECTEURS PUBLICS ET PRIVÉS, MAIS LA MASSE DES ACTEURS N'EST PAS ENCORE PRIORITAIRE

Au cours des quinze dernières années, et en particulier depuis 2015, la puissance publique a multiplié les initiatives pour prendre en compte et s'adapter à l'intensification de la menace cyber, et accompagner les différentes couches d'utilisateurs ou de victimes.

Éventail des dispositifs mis en place en France dans la période récente

Année	Type	Nom)	Description
2010/ 2014	Normatif	Référentiel général de sécurité[64] (RGS)	Le RGS est un ensemble de règles de sécurité numérique visant à instaurer la confiance dans les échanges entre autorités administratives et entre les administrations et les citoyens.
2015	Stratégique	Stratégie nationale pour la sécurité numérique	Renforcement de la sécurité des OIV, des entreprises non OIV, apprentissage de la sécurité numérique dans toute formation et dès l'école, filière de cybersécurité, action internationale.

[64] *https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/*

Année	Type	Nom)	Description
2015	Stratégique	Stratégie ministérielle de lutte contre les cybermenaces	Défendre les intérêts, assurer la confiance numérique, assurer la prévention sur les territoires, favoriser la politique industrielle, contribuer à la souveraineté numérique
2017	Institutionnel	GIP ACYMA (Cybermalveillance.gouv.fr)	Assistance aux victimes de cybercriminalité (particuliers, entreprises non régulées, associations, collectivités)
2017	Pédagogique	SecNumAcadémie[65] de l'ANSSI	MOOC (Massive Open online Course) visant à initier le grand public à la cybersécurité.
2020	Pédagogique	Programme de sensibilisation aux risques numériques dans les collectivités territoriales[66] (Cybermalveillance.gouv.fr)	Programme de sensibilisation en matière de sécurité numérique à destination des élus coordonné par ACYMA avec la participation de l'AMF, de l'ANSSI, de l'ANCT, de l'APVF, de l'AVICCA, de la Banque des Territoires, du CoTer Numérique, de Déclic, du ministère de l'Intérieur, des Régions de France et de la Région Pays de la Loire.
2020	Investissement	Volet cybersécurité du plan France Relance (cf. section ci-dessous) doté de 176M€	Cofinancement de projets et de parcours de cybersécurité, via un guichet de tenu par l'ANSSI, à destination de collectivités territoriales, d'hôpitaux et d'établissements publics **(800 bénéficiaires jusqu'à ce jour dont environ 600 collectivités, pour 45 000 collectivités locales)**[67] Licences mutualisées pour les collectivités les plus petites ne pouvant bénéficier des parcours de cybersécurité[68] Mise en place d'un réseau de CSIRT régionaux[69]

[65] https://secnumacademie.gouv.fr/
[66] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/programme-sensibilisation-risques-numeriques-collectivites-territo riales#
[67] https://www.ssi.gouv.fr/agence/cybersecurite/france-relance/parcours-de-cybersecurite/
[68] https://www.ssi.gouv.fr/actualite/lancement-dun-nouveau-dispositif-france-relance-au-profit-des-collectivites-territoriales/
[69] https://www.cert.ssi.gouv.fr/csirt/csirt-regionaux/

Année	Type	Nom)	Description
2017	Investissement	Stratégie nationale d'accélération pour la cybersécurité (financée à hauteur de 1 Md€), rattachée au plan France 2030 et incluant le volet cybersécurité du plan France Relance	Cf. ci-dessous
2021	Institutionnel	Dispositif "Alerte-Cyber" (Cybermalveillance.gouv.fr/ANSSI)	Le dispositif AlerteCyber est un système d'alerte en France qui vise à aider les TPE/PME à se protéger contre les attaques cyber. Il consiste en la diffusion rapide, par l'intermédiaire des organisations interprofessionnelles et des réseaux consulaires, de bulletins d'alerte relatifs à des vulnérabilités susceptibles de toucher un grand nombre de petites entreprises. Ledit bulletin fournit un descriptif simplifié de la vulnérabilité et des mesures à prendre pour se protéger, en complément des bulletins du CERT-FR destinés aux experts en cybersécurité. Le dispositif a récemment été mobilisé dans le cadre de la campagne d'attaques par chaîne d'approvisionnement impliquant le client de la solution VoIP 3CX[70].
2022	Normatif	Loi du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public	Cette loi (également appelée loi Lafon) rend obligatoire pour les plateformes numériques (cloud, etc.), à partir du er octobre 2023, la réalisation d'un audit de cybersécurité portant sur la sécurisation et la localisation des données. Cet audit aboutira, pour chaque plateforme, à l'obtention d'un **cyberscore** permettant au grand public de classer les différentes plateformes entre elles.

[70] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/compromission-de-lapplication-3cx-electron-desktop-app

Année	Type	Nom)	Description
2022	Normatif	Mon service sécurisé[71]	Service gratuit et collaboratif, incubé par le laboratoire d'innovation de l'ANSSI, visant à renforcer la cybersécurité de tous les services publics numériques (téléservices) : site web, applications mobiles et API. Cet outil a pour vocation à aider les collectivités et les administrations à obtenir l'homologation de leurs téléservices, obligatoire au titre du RGS.
2023	Normatif	Loi LOPMI[72] (volet cyber) du 23 janvier 2023[73]	Afin de permettre une meilleure information de la police et de la justice, à partir d'avril 2023. Il est inséré un nouvel article L. 12-10-111 dans le code des assurances qui subordonne le versement d'une somme en application de la clause d'un contrat d'assurance visant à indemniser un assuré des pertes et dommages causés par une atteinte à un système de traitement automatisé de données mentionnée aux articles 323-1 à 323-3-1 du code pénal au dépôt d'une plainte de la victime. L'aggravation des peines en cas de cyberattaques menées à l'encontre d'un réseau informatique ou bancaire, d'un hôpital ou d'un service d'appels d'urgence est prévue. Le gouvernement devra remettre d'ici fin 2023 deux rapports évaluant la protection des collectivités locales et des entreprises face aux cyberattaques.

[71] https://www.ssi.gouv.fr/actualite/monservicesecurise-une-nouvelle-solution-de-lanssi/
[72] *Loi d'orientation et de programmation du ministère de l'intérieur*
[73] https://www.vie-publique.fr/loi/284424-loi-24-janvier-2023-securite-lopmi-programmation-ministere-interieur

Année	Type	Nom)	Description
2023	Outil / Service	Bouclier cyber	Une plateforme de services mutualisés sur la base d'un abonnement pour permettre aux collectivités de bénéficier d'un nom de domaine, d'une messagerie et d'un hébergement en ligne sécurisés Outil d'autodiagnostic et d'audit gratuit à destination des entreprises Filtre anti-arnaque à destination des particuliers pour bloquer les sites réputés afficher du contenu malveillant

La stratégie nationale d'accélération cyber, lancée en février 2021 et ensuite rattachée au plan d'investissement France 2030, a fléché une partie de ses moyens vers la cybersécurité des administrations, des collectivités et des établissements de santé (axe 3 de la stratégie - cf. encadré ci-dessous). Sur la période 2021-2022, **sous le pilotage de l'ANSSI, 176M€, initialement rattachés au volet cybersécurité du plan France Relance, ont été répartis** entre :

- des parcours de cybersécurité[74] , à hauteur de 100M€ (plus de détails sur leurs bénéficiaires et leur fonctionnement en annexe 5) ;
- des appels à projet[75] , pour un montant de 27M€, à destination de petites collectivités et d'autres entités (collectivités matures, ministères et autres réseaux de l'État, selon un schéma de cofinancement) non éligibles aux parcours de cybersécurité ;
- le soutien à la création des CSIRT (*computers security incident response teams*) régionaux, à hauteur de 1M€ par CSIRT, qui sont des centres

[74] *Visant à élever significativement et rapidement le niveau de sécurité numérique de 946 bénéficiaires parmi lesquels 710 collectivités (des collectivités de plus de 10 000 habitants essentiellement), 133 établissements de santé et 103 établissements publics.*
[75] *Incluant 5,2M€ pour l'acquisition de licences mutualisées qui sont distribuées aux petites collectivités.*

d'alerte et de réaction aux attaques informatiques destinés à traiter les demandes d'assistance des acteurs de taille intermédiaire (entreprises, collectivités territoriales et associations) et faire l'interface avec les prestataires locaux de réponse à incidents ;

- le développement et le déploiement mutualisés de capacités nationales de cybersécurité.

La stratégie nationale d'accélération cyber

La stratégie nationale d'accélération cyber, lancée en février 2021 avant d'être rattachée au plan d'investissement France 2030, mobilise un peu plus d'un milliard d'euros (dont 720 M€ de financements publics) pour atteindre trois objectifs clés à horizon 2025 :

- un chiffre d'affaires de 25 Mds€ pour la filière (x3 par rapport à la situation actuelle) ;
- le doublement des emplois dans le secteur (en passant de 37 000 à 75 000 emplois) ;
- l'émergence de trois licornes françaises en cybersécurité.

Pour atteindre ces objectifs, cette stratégie s'articule autour des 5 axes suivants :

- **Axe 1 :** développer des solutions souveraines et innovantes de cybersécurité, en finançant des appels à projets pour développer la filière française, à hauteur de 250M€ et en soutenant la recherche, notamment par l'intermédiaire d'un programme équipement prioritaires de recherche (PEPR) doté de 65M€ ;

- **Axe 2** : renforcer les liens et synergies entre les acteurs de la filière, avec notamment la création du Campus Cyber dans le quartier de La Défense, bénéficiant de 100M€ de financements directs ou indirects ;

- **Axe 3** : soutenir la demande (individus, entreprises, collectivités et État), notamment en renforçant la cybersécurité des administrations et des collectivités par l'intermédiaire du volet cybersécurité du plan France Relance mobilisant 136M€ (montant porté ultérieurement à 176M€) sur la période 2021-2022, sous le pilotage de l'ANSSI ;

- **Axe 4** : former plus de jeunes et professionnels aux métiers de la cybersécurité, avec un financement de 140M€ via l'appel à manifestation d'intérêt "Compétences et métiers d'avenir" ;

- **Axe 5** : soutenir le développement des entreprises *via* des investissements en fonds propres.

Synthèse des montants de la stratégie nationale cyber[76]

En M€	Développer des solutions souveraines	Renforcer les synergies	Soutenir l'adoption de solutions cyber	Soutien en fonds propres	Total
Part publique	290	74	156	200 (prévisionnel)	720
Part privée	225	74	20	n.a.	> 319
Financement	515	148	176	200	> 1039

[76] *Nouveaux crédits hors militaires et formation. Source : https://www.entreprises.gouv.fr/fr/strategies-d-acceleration/strategie-d-acceleration-cybersecurite*

D'après la Banque européenne d'investissement[77], la France et l'Allemagne sont les États membres investissant le plus dans leur cybersécurité. Lorsqu'il était encore membre, le Royaume-Uni était le pays européen investissant le plus.

Au niveau de l'Union européenne, en complément de la directive NIS 2 adoptée en novembre 2022 (cf. *supra*), le projet de règlement *Cyber Resilience Act* amorce un début de réflexion en matière de passage à l'échelle en renforçant la cybersécurité des produits numériques commercialisés sur le marché intérieur.

[77] https://www.eib.org/attachments/lucalli/20220206-european-cybersecurity-investment-platform-en.pdf

Le règlement européen *Cyber Resilience Act*

Fondé sur la Stratégie de cybersécurité européenne établie en 2020, et dans la continuité du règlement *Cyber Security Act* adopté en mars 2019, le projet de règlement *Cyber Resilience Act*, présenté par la Commission européenne le 15 septembre 2022[78] et toujours en cours de rédaction, vise à renforcer la cybersécurité des produits numériques commercialisés sur le marché intérieur.

Pour ce faire, le règlement souhaite mettre en place un cadre commun de normes minimales en matière de cybersécurité et imposera aux fabricants, d'une part, de renforcer l'information des utilisateurs pour leur permettre d'évaluer le niveau de cybersécurité d'un produit et, d'autre part, d'assurer la sécurité numérique de leurs produits tout au long de leur cycle de vie.

Ce cadre européen imposerait également des normes plus strictes pour certains produits jouant un rôle central dans la

[78] https://digital-strategy.ec.europa.eu/fr/library/cyber-resilience-act

sécurité des réseaux ou susceptibles de présenter des vulnérabilités affectant un grand nombre d'utilisateurs, comme les systèmes d'exploitation, les hyperviseurs, les antivirus, les gestionnaires de mots de passe, ou les objets connectés destinés au secteur industriel.

Les fabricants des produits numériques les plus critiques seront de plus tenus de signaler à l'Agence de l'Union européenne pour la cybersécurité (ENISA) les nouvelles vulnérabilités découvertes au sein des produits, dans un délai de 24 heures. En cas de non-respect des nouvelles règles de cybersécurité, les entreprises s'exposeraient à des amendes pouvant s'élever à 15 M€ ou 2,5 % de leur chiffre d'affaires mondial.

Jusqu'à présent, la législation actuelle traitant du marché intérieur s'applique seulement à certains produits contenant des éléments numériques, mais la majorité des produits ne sont pas couverts par la législation en matière de cybersécurité. Par exemple, le cadre juridique actuel n'évoque pas le cas des logiciels non intégrés.

Ainsi, la Commission européenne définit deux objectifs principaux pour tenir compte de ces aspects dans le fonctionnement du marché intérieur:

- "*créer les conditions nécessaires au développement de produits sûrs comportant des éléments numériques en veillant à ce que les produits matériels et logiciels soient mis sur le marché avec moins de vulnérabilités et veiller à ce que les fabricants prennent la sécurité au sérieux tout au long du cycle de vie d'un produit*";

- "*créer des conditions permettant aux utilisateurs de tenir compte de la cybersécurité lors de la sélection et de l'utilisation de produits comportant des éléments numériques.*"

Au-delà de ces axes principaux, des objectifs plus spécifiques ont également été définis :

- "*veiller à ce que les fabricants améliorent la sécurité des produits comportant des éléments numériques depuis la phase de conception et de développement et tout au long du cycle de vie*";
- "*garantir un cadre cohérent en matière de cybersécurité, en facilitant le respect des règles par les producteurs de matériel et de logiciels*";
- "*améliorer la transparence des propriétés de sécurité des produits comportant des éléments numériques, et permettre aux entreprises et aux consommateurs d'utiliser des produits comportant des éléments numériques en toute sécurité.*"

I.7. PARANGONNAGE INTERNATIONAL : DANS LE MONDE, CERTAINS PAYS ONT SU GÉNÉRALISER UN NIVEAU MINIMUM DE CYBERSÉCURITÉ, AVEC DES RÉSULTATS PROBANTS

Face à la hausse de la menace cyber ciblant tout particulièrement les petites structures telles que les TPE/PME ou les collectivités, il est intéressant de comprendre comment ont réagi d'autres pays. A ce titre, d'après les experts, les États-Unis et Israël font partie des pays les plus avancés. En Europe, le Royaume-Uni semble une référence (bien que n'étant plus membre de l'Union) et l'Allemagne constitue un point de comparaison utile avec la France, tandis que l'Estonie présente une antériorité intéressante en matière de risque systémique de cyberattaque.

S'agissant du haut du spectre (grands groupes, entreprises stratégiques), **la France[79] , le Royaume-Uni et l'Estonie ont été en mesure d'imposer des mesures de cybersécurité à des opérateurs d'infrastructure critiques** pour la bonne marche de leur nation, notamment avec la directive européenne NIS de 2016. **Les diverses tentatives initiées aux États-Unis visant à légiférer sur la cybersécurité des infrastructures critiques nationales ont paru moins abouties.**

En effet, la compétence du gouvernement fédéral des États-Unis en matière de cybersécurité est circonscrite à la protection des réseaux fédéraux et repose, d'une part, sur la NSA (*National Security Agency*), également en charge d'activités cyber offensives et plus généralement de la collecte du renseignement technique auprès des puissances étrangères (ce qui n'est pas sans soulever des questions de confiance) pour les réseaux fédéraux classifiés et, d'autre part, la CISA (*Cybersecurity and Infrastructure Security Agency*) pour les réseaux non classifiés et les compétences de coordination et de politique de sécurité. La responsabilité d'assurer la cybersécurité des administrations incombe ainsi à celles-ci.

S'il existe quelques réglementations sectorielles portées par des autorités de régulation, il n'existe pas, à proprement parler, de législation nationale visant à garantir la cybersécurité des infrastructures critiques qui seraient portées par des entreprises. Notons que la nouvelle stratégie affiche des objectifs volontaristes en la matière, qui pourraient engendrer de nouvelles obligations.

Néanmoins, le gouvernement fédéral est récemment parvenu à faire aboutir quelques initiatives[80]. En mars 2023, l'administration Biden a publié une nou-

[79] *A partir de 2013 avec le Livre blanc sur la défense et la sécurité nationale et la Loi de programmation militaire (LPM).*

[80] *Ainsi, à l'issue de l'attaque par rançongiciel ayant ciblé Colonial Pipeline le 7 mai 2021, le président des États-Unis a signé, en mai 2021, un décret obligeant les fournisseurs de services informatiques d'informer le gouvernement des cyberattaques susceptibles d'affecter les réseaux nationaux.*

velle stratégie nationale en matière de cybersécurité (*National Cybersecurity Strategy*, rédigée par le nouvel *Office of the National Cyber Director*, directement rattaché au président américain depuis le 1er janvier 2021) pouvant déboucher sur une nouvelle législation qui obligerait les entreprises à mettre en œuvre des mesures minimales de cybersécurité pour les infrastructures critiques, et ouvrirait la voie à l'engagement de responsabilité des entreprises qui ne parviennent pas à sécuriser le code des produits numériques qu'ils commercialisent[81]. Cette initiative pourrait entraîner des effets vertueux majeurs, dans la mesure où de nombreux grands éditeurs numériques sont américains.

Au sein de l'Union, si la France fut précurseur grâce à la LPM de 2013 avec la notion d'opérateur d'importance vitale (OIV) et la consécration du rôle de l'ANSSI en tant qu'autorité nationale compétente pour la réception voire le traitement des incidents remontés par ces acteurs critiques, le Royaume-Uni et l'Estonie s'étaient eux aussi dotés très tôt de structures de réponse nationale, respectivement avec le NCSC-UK (*National CyberSecurity Center*) et le CERT-EE, pour être en mesure de répondre aux cyberattaques ciblant les infrastructures critiques.

Concernant le bas du spectre, les différents pays du panel étudié semblent tous disposer d'autorités gouvernementales chargées du suivi des petites structures (PME, petites collectivités) victimes de cyberattaques. Comme le montre le tableau ci-dessous, certains pays disposent d'autorités spécifiquement dédiées à l'assistance des petites entités (les États-Unis, la France dans une certaine mesure) tandis que la majorité (Allemagne, Estonie, Royaume-Uni, Israël) ont fait le choix de regrouper sous une même autorité la mission de défense des infrastructures critiques et d'assistance aux petites entreprises et collectivités.

[81] *"We must [...] reshape laws that govern liability for data losses and harm caused by cybersecurity errors, software vulnerabilities, and other risks created by software and digital technologies".*

<table>
<tr><th>En M€</th><th colspan="2">Haut du spectre (assistance aux infrastructures critiques)</th><th>Bas du spectre (assistance aux petites et moyennes entreprises)</th><th>Réponse judiciaire</th></tr>
<tr><td>France</td><td colspan="2">Agence nationale de la sécurité des systèmes d'information (ANSSI)

Et dans une certaine mesure: services de renseignement du premier cercle</td><td>Cybermalveillance.gouv.fr

Et dans une certaine mesure: Commandement de la gendarmerie dans le cyberespace, Police nationale, Préfecture de police, services de renseignement</td><td>Commandement de la gendarmerie dans le cyberespace (ComCyberGend)

Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)

Brigade de lutte contre la cybercriminalité (BL2C)</td></tr>
<tr><td>États-Unis</td><td>Systèmes classifiés</td><td>Systèmes non classifiés</td><td rowspan="2">Cyber Division du FBI, Internet Crime Complaint Center (IC3)</td><td>Cyber Division, Federal Bureau of Investigation (FBI)

United States Secret Service

Department of Justice Computer Crime and Intellectual Property Section (CCIPS)</td></tr>
<tr><td rowspan="2">Allemagne</td><td>National Security Agency (NSA)</td><td>Cybersecurity and Infrastructure Security Agency (CISA)</td><td></td></tr>
<tr><td colspan="3">Bundesamt für Sicherheit in der Informationstechnik (BSI)</td><td>Bundeskriminalamt (BKA)</td></tr>
<tr><td>Estonie</td><td colspan="3">CERT-EE, Estonian Information System Authority (RIA)</td><td>Politsei- ja Piirivalveamet (PPA)</td></tr>
<tr><td>Royaume-Uni</td><td colspan="3">Centre national de cybersécurité (NCSC-UK)</td><td>National Crime Agency (NCA)
National Cyber Crime Unit</td></tr>
<tr><td>Israël</td><td colspan="3">CERT-IL, National Cyber Security Directorate (INCD)</td><td>Lahav 433 (Unité nationale de lutte contre la cybercriminalité)</td></tr>
</table>

L'autorité en question est rattachée à un service de renseignement .

Aux États-Unis, l'*Internet Crime Complaint Center* (IC3) est une division du FBI créée en mai 2000 qui traite les plaintes pour les infractions liées à l'Internet et aux technologies de l'information. En remplissant un formulaire de plainte en ligne, les victimes, particuliers comme entreprises, peuvent signaler des escroqueries en ligne, des fraudes bancaires, des piratages de comptes de messagerie ou de réseaux sociaux, des rançongiciels, etc. Les signalements remontés permettent à l'IC3 d'identifier les grandes tendances en matière de cybercriminalité et de déployer des ressources pour lutter contre ces menaces en prenant en compte l'incident, après analyse, au juste niveau de traitement.

Certaines de ces autorités nationales dédiées à l'assistance des entités non sensibles proposent des programmes de sensibilisation, d'accompagnement, voire de labellisation à destination des petites et moyennes entreprises :

- En France, l'ANSSI[82] et Cybermalveillance.gouv.fr[83] produisent différents contenus formulant des pistes de recommandations pour aider les TPE/PME à se protéger contre les menaces en ligne. La gendarmerie nationale conduit des actions évoquées au titre de l'étude de terrain (p. 64). La police nationale anime un réseau de référent cybermenaces[84], qui réalisent notamment des actions de sensibilisation auprès du tissu économique local ;
- En Allemagne, le BSI propose un programme appelé "*Allianz für Cyber-Sicherheit*"[85] (Alliance pour la cybersécurité) afin d'aider les petites et moyennes entreprises à améliorer leur posture de cybersécurité ;

[82] https://www.ssi.gouv.fr/guide/la-cybersecurite-pour-les-tpepme-en-treize-questions/

[83] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybersecurite-tpe-pme-enjeux-solutions

[84] *Le réseau des référents cybermenaces (RCM) de la Police nationale est composé de commissaires de police, pour guider le tissu économique et le réseau institutionnel dans le processus de contact et de prise de plainte, de policiers spécialisés dans l'investigation numérique, de réservistes citoyens, issus du secteur privé, qui s'engagent dans la prévention des cybermenaces. Le réseau conduit des actions pour sensibiliser le tissu économique local au risque cyber à travers des outils de communication spécifiques, et mettre en place un point de contact territorial dédié aux entreprises (permettant d'obtenir des informations, poser des questions), mais également de prendre rendez-vous en cas d'infraction.*

[85] https://www.allianz-fuer-cybersicherheit.de

- Au Royaume-Uni, le NCSC-UK propose également gratuitement une série d'outils et de services de cybersécurité aux organisations éligibles dans le cadre du programme *Active Cyber Defence* (ACD)[86]. Ce programme inclut notamment un service de résolution DNS (*Protective Domain Name Service*) et un service de scan externe des vulnérabilités pour les adresses IP exposées sur Internet (*Early Warning Service*). En outre, le NCSC-UK a lancé un **système de labellisation** appelé "*Cyber Essentials*" qui fournit des conseils et une assistance aux petites et moyennes entreprises pour améliorer leur posture de cybersécurité. Les entreprises peuvent obtenir une certification *Cyber Essentials* prouvant qu'elles ont mis en place des mesures de sécurité de base pour se protéger contre les cyberattaques courantes.

Afin de comparer la charge de ces différentes autorités administratives chargées de prêter assistance aux entreprises hors infrastructures critiques, une méthode de première approximation pourrait consister à calculer le ratio, par pays, entre le nombre d'attaques par rançongiciels déclarées par les entreprises (auprès des différentes autorités compétentes ou de plateformes d'identification de souches de rançongiciels) et le nombre d'entreprises.

Dans cette perspective, le tableau ci-dessous présente, pour la France, les États-Unis, le Royaume-Uni, Israël et l'Estonie, le nombre d'attaques par rançongiciels déclarées, toutes entités confondues[87] (entreprises, collectivités, établissements de santé et particuliers), auprès des différentes autorités compétentes[88], le nombre d'entreprises (comptant au moins un employé), ainsi que le nombre d'interrogations (hors particuliers) sur la plateforme d'identification de rançongiciel "ID Ransomware", sur laquelle est fondée l'étude Emsisoft (cf. annexe 3 - déjà mentionnée).

[86] https://www.ncsc.gov.uk/section/active-cyber-defence/introduction

[87] *Il n'a pas été possible de trouver le nombre d'attaques par rançongiciels uniquement déclarées par les entreprises pour les différents pays du panel de comparaison, hormis la France.*

[88] *Sauf pour l'Allemagne où, en l'absence de "chiffres officiels", des données sont celles de l'entreprise Recorded Future.*

	Interrogations distinctes sur la plateforme "Ransomware ID"	Attaques par rançongiciels déclarées (en 2020)	Attaques par rançongiciels déclarées (en 2021)	Nombre d'entreprises avec au moins 1 employé
France	4476 (Emsisoft)	~1000 (ACYMA[89])	~1945 (ACYMA[90])	~1,5 M (INSEE, 2021)
États-Unis	15672 (Emsisoft)	2474 (IC3[91])	3729 (IC3[92])	~7,7 M (SBA, 2021)
Israël	/	138 (INCD, moy.19-21[93])	138 (INCD, moy.19-21[94])	~280 K (BCS, 2021)
Royaume-Uni	2718 (Emsisoft)	326 (NCSC-UK[95])	654 (NCSC-UK[96])	~1,4 M (ONS 2021)
Estonie	/	21 (RIA[97])	30 (RIA[98])	~50 K (Statistikaamet, 2021)
Allemagne	3747 (Emsisoft)	60 (Recorded Future[99])	110 (Recorded Future[100])	~2 M (Destatis, 2021)

[89] https://www.cybermalveillance.gouv.fr/medias/2022/03/cybermalveillance-rapport-activite-2021.pdf
[90] https://medias.vie-publique.fr/data_storage_s3/rapport/pdf/288757.pdf
[91] https://first-response.co.uk/articles/uk-and-us-cybercrime-statistics/
[92] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
[93] https://barlaw.co.il/client-updates/ransomware-attacks-new-israeli-justice-ministry-recommendations
[94] https://barlaw.co.il/client-updates/ransomware-attacks-new-israeli-justice-ministry-recommendations
[95] https://first-response.co.uk/articles/uk-and-us-cybercrime-statistics/
[96] https://first-response.co.uk/articles/uk-and-us-cybercrime-statistics/
[97] https://e-estonia.com/in-2022-estonia-had-the-highest-number-of-cyber-attacks/ 97 https://e-estonia.com/in-2022-estonia-had-the-highest-number-of-cyber-attacks/
[98] https://www.recordedfuture.com/germany-industrial-sector-hit-hardest-by-ransomware-in-2020-2021
[99] https://www.recordedfuture.com/germany-industrial-sector-hit-hardest-by-ransomware-in-2020-2021
[100] https://www.recordedfuture.com/germany-industrial-sector-hit-hardest-by-ransomware-in-2020-2021

Ces chiffres sont à considérer avec prudence pour deux raisons :

- Tout d'abord, ceux-ci recouvrent, en fonction du pays, une réalité différente : demande d'assistance contre rançongiciel, signalement, plainte ou interrogation d'un site d'identification de souches de rançongiciels. En particulier, si les chiffres donnés par Cybermalveillance.gouv.fr pour la France s'appuient sur le nombre de recherches d'assistance sur les attaques par rançongiciel soumises sur la plateforme, les chiffres de l'IC3 américain s'appuient sur des déclarations d'incidents en bonne et due forme remplies par les victimes.

- En outre, les chiffres liés au nombre d'attaques déclarées en 2020 et 2021 sont par nature biaisés dans le sens où, en fonction du pays, les entreprises et les collectivités locales sont plus incitées dans d'autres pays à déclarer (ou signaler) les incidents dont ils font l'objet. À cet égard, il est intéressant de constater l'écart, pour différents pays, entre le nombre d'interrogations distinctes sur la plateforme "Ransomware ID" (quand ils sont disponibles) et le nombre d'attaques déclarées auprès des autorités administratives compétentes.

2 Le faible niveau de cybersécurité de la grande majorité d'acteurs, en particulier les TPE/PME/ETI et collectivités, s'explique par plusieurs raisons et facteurs aggravants

II.1. RAISON 1 : LA SURFACE D'ATTAQUE EST PLUS GRANDE

En premier lieu, le nombre d'outils et de systèmes numériques en circulation en France a fortement augmenté, de même que le volume des données en circulation[100]. Les dispositifs de sécurité ont suivi, de manière *ad hoc* et quelque peu anarchique. Dans le même temps, la façon d'utiliser ces outils et systèmes a évolué et le temps d'utilisation a nettement augmenté, le télétravail venant accentuer cette évolution.

De plus, de nombreuses TPE/PME/ETI ont procédé à l'externalisation de tout ou partie de leur infrastructure informatique (*cloud computing*) auprès d'entreprises de services numériques (ESN). Si les ESN proposent des niveaux de sécurité plus élevés en moyenne qu'une infrastructure numérique développée en interne, la compromission d'une ESN peut entraîner, de manière indirecte, la compromission de l'ensemble des entreprises dont le système d'information est hébergé chez cet ESN, induisant un effet d'échelle[101]. Ainsi, en juillet 2021, la compromission par le groupe REvil de Keseya, entreprise éditant une suite intégrée de gestion des infrastructures informatiques à destination des entreprises moyennes, a conduit au déploiement d'un rançongiciel chez un peu plus de 1 000 entreprises clientes de cet ESN[102]. L'exemple de l'administration Suisse atteinte par une cyberattaque à travers son fournisseur informatique Xplain est marquante, nul n'étant à l'abri.

[101] https://fr.statista.com/infographie/17800/big-data-evolution-volume-donnees-numeriques-genere-dans-le-monde/
[102] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf
[103] https://en.wikipedia.org/wiki/Kaseya_VSA_ransomware_attack

Les offres les plus sécurisées sont souvent les plus chères, et les petites structures (qui relativisent le risque faute de le connaître ou de se sentir concernés) font souvent le choix de l'investissement à moindre coût. Le choix du fournisseur informatique et de la bonne offre de service sont donc clés.

II.2. RAISON 2 : UN MANQUE DE SENSIBILISATION

Selon une étude d'Ipsos de novembre 2022, les deux tiers des salariés français n'ont jamais reçu la moindre formation à la cybersécurité[104]. Près de la moitié des entreprises françaises (45 %) ne proposent aucune formation de sensibilisation, quels que soient les postes dans l'entreprise. 79 % des personnes interrogées dans le cadre de l'étude estiment pourtant qu'une sensibilisation à la cybersécurité pourrait les intéresser. Leur niveau de conscience du risque est faible, puisque 52 % des salariés interrogés estiment encore que leur emploi n'a absolument rien à voir avec la cybersécurité et que leurs actions (involontaires ou pas) n'ont pas d'impact sur la sécurité de leur entreprise.

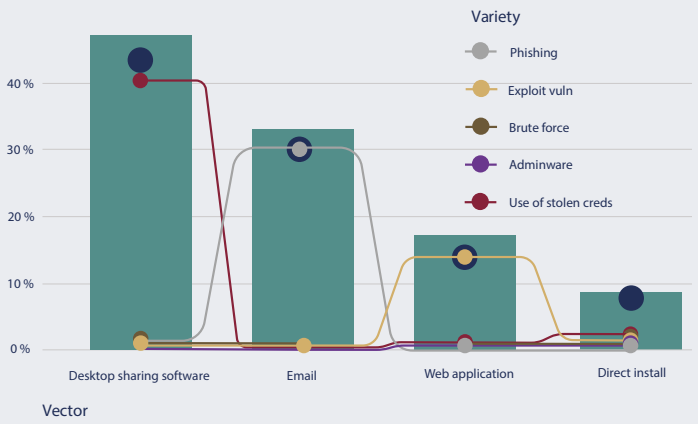
Pourtant, dans environ la moitié des cas[105], c'est une action de l'utilisateur final qui permet à un attaquant de pénétrer dans le système ciblé, les erreurs de configuration ou de programmation pouvant représenter le reliquat. En effet, selon le rapport d'enquêtes sur les violations de données de 2022 de Verizon[106], les vecteurs d'intrusion initiale afférents à une compromission par rançongiciel ont été :

- **dans 40 % des cas, l'utilisation d'identifiants volés** (résultant généralement de la compromission initiale d'un partenaire pouvant résulter d'une erreur humaine) pour accéder à un système de partage de bureau à distance tel que *Remote Desktop Protocol* ;
- **dans 35 % des cas, le recours à des courriels d'hameçonnage** pour faire exécuter par l'utilisateur une charge malveillante sur un poste du réseau ciblé ;

[104] https://www.lefigaro.fr/secteur/high-tech/cyberattaques-62-des-francais-n-ont-jamais-recu-une-formation-a-la-securite-informatique-20221025
[105] https://www.netexplorer.fr/blog/cyberattaque-facteur-humain-responsable-de-80-des-cas/
[106] https://www.verizon.com/business/resources/Tcfe/reports/dbir/2022-data-breach-investigations-report-dbir.pdf

- dans 15 % des cas, **l'exploitation d'une vulnérabilité sur une application web** interconnectée avec le réseau de la cible.

Les vecteurs d'intrusion initiale afférents à une compromission par rançongiciel



Source : Data Breach Investigations Report, Verizon (2022)[107]

Enfin, d'après une étude de Cybermalveillance.gouv.fr, réalisée en 2022, **65 % des collectivités de moins de 3 500 habitants pensent que le risque en matière de cybersécurité est faible, voire inexistant, ou ne savent pas l'évaluer**[108].

Or, comme indiqué, le risque provient à la fois de compromissions humaines (primo-infection due à des erreurs humaines) et de compromissions de systèmes (à travers les connexions avec d'autres services, d'autres prestataires,

[107] https://www.verizon.com/business/resources/Tcfe/reports/dbir/2022-data-breach-investigations-report-dbir.pdf
[108] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/etude-cybersecurite-collectivites-moins-de-3500-habitants

par exemple). Les petites entreprises et les collectivités doivent prendre en compte ces deux dimensions et ne pas s'exonérer en pensant que cela n'arrive qu'aux autres ou aux imprudents.

En matière de sensibilisation au risque cyber, l'ANSSI et Cybermalveillance.gouv.fr publient régulièrement des guides et des recommandations pratiques sur la cybersécurité. Ces documents fournissent des conseils et des bonnes pratiques aux utilisateurs, aux entreprises et aux organisations pour les aider à renforcer leur sécurité informatique (certains de ces guides sont mentionnés en annexe 8).

L'ANSSI propose également, depuis mai 2017, le MOOC (Massive Open Online Course) "SecNumAcadémie" qui vise à sensibiliser et former le plus grand nombre d'individus aux enjeux et aux bonnes pratiques en matière de cybersécurité. En 2021, 200 000 apprenants s'étaient inscrits (306 101 en 2023) et 35 000 seulement avaient obtenu l'attestation de réussite du MOOC en suivant les 8 heures de formation jusqu'au bout.

De son côté, Cybermalveillance.gouv.fr mène aussi des actions de sensibilisation auprès du grand public, des entreprises et des collectivités par l'intermédiaire de publications, de campagnes de communication, d'interventions dans des événements et des formations pour informer les utilisateurs sur les risques liés à la cybersécurité et les moyens de s'en protéger.

II.3. RAISON 3 : LES MONTANTS INVESTIS DANS LA CYBERSÉCURITÉ N'ONT PAS ÉTÉ À LA HAUTEUR DES BESOINS

La part du budget numérique des entreprises dédiée à la cybersécurité est souvent faible en dehors des grandes entreprises (et entreprises vitales/essentielles), et dépend parfois du fait d'avoir déjà été victime de cyberattaque ou non. Pour les entreprises, le fait de disposer de systèmes robustes en matière de cybersécurité n'est pas strictement nécessaire à leur réussite économique; toute ressource investie dans la cybersécurité n'est pas directement consacrée à leurs activités profitables et par conséquent l'incitation n'est pas favorable à une bonne considération de la menace cyber.

D'après une étude de l'IFOP avril 2021 portant à 75 % sur des PME[109], **60 % des entreprises françaises consacrent moins de 1 000€ par an à la cybersécurité, alors que l'ANSSI recommande d'y consacrer au moins 5 % du budget IT[110] et les experts de la filière 10 %.** Dans un contexte inflationniste, les montants alloués à la cybersécurité ont par ailleurs tendance à être réduits[111].

Dans les collectivités, les freins aux investissements dans la cybersécurité sont, d'une part, d'ordres financiers, et d'autre part, résultent d'une méconnaissance juridique.

II.4. RAISON 4 : UN MANQUE DE COMPÉTENCES DISPONIBLES DANS UN MARCHÉ TENDU

Selon une note de l'Institut Montaigne de mai 2023, les métiers de la cybersécurité sont les plus tendus des métiers du numérique[112]. **Les besoins de recrutement ont doublé en 5 ans[113]**, confrontés à un manque chronique de talents pour les satisfaire. Plus de 15 000[114] postes étaient vacants en mars 2022 et **seulement 25 % des offres d'emploi pourvues en 2021[115]**, alors que les écoles françaises ne forment qu'environ 400 diplômés par an dans le domaine de la cybersécurité[116]. **Les métiers de la cybersécurité restent encore largement méconnus et sous-investis.**

[109] https://itrnews.com/articles/190035/f-secure-decortique-le-rapport-quentretiennent-les-entreprises-et-les-particuliers-avec-la-cybersecurite.html

[110] *Ces budgets ne couvrent généralement pas la question de la sensibilisation ou de la formation, mais les outils et solutions, ainsi que les compétences spécialisées.*

[111] *D'après l'ENISA, la part dédiée à la cybersécurité au sein des budgets IT des opérateurs essentiels de l'UE est passée de 7,7 % à 6,7 % en médian et de 8,8 % à 7,2 % en moyenne (entre 2021 et 2020).*

[112] https://www.institutmontaigne.org/publications/mobiliser-et-former-les-talents-du-numerique

[113] https://corporate.apec.fr/files/live/sites/corporate/files/Nos%20%C3%A9tudes/pdf/cybersecurite-un-marche-de-lemploi-cadre-diversifie-et-de-pl us-en-plus-porteur#:~:text=Aussi%2C%20le%20volume%20des%20offres,650%20%C3%A0%207%20000%20offres.

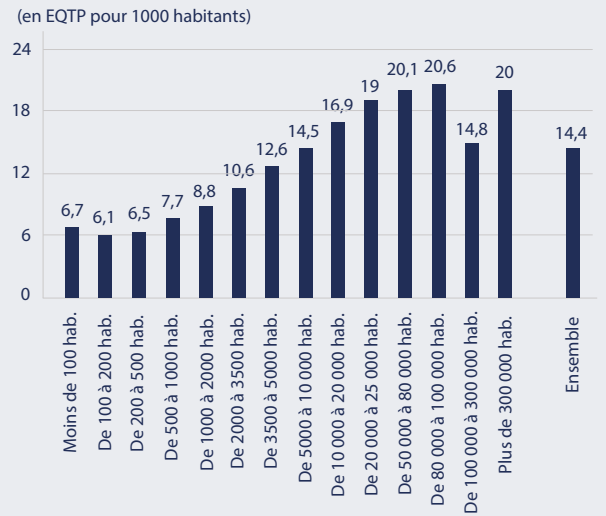
[114] https://www.wavestone.com/fr/communiques-de-presse/cybersecurite-ou-en-sont-les-grandes-organisations-francaises/

[115] https://www.emploiparlonsnet.pole-emploi.org/articles/la-cybersecurite-une-filiere-davenir/

[116] https://incyber.org/cyber-se-perdra-faute-de-combattants/

Face aux moyens des grandes entreprises et aux tensions concurrentielles, les petites et moyennes structures ont **peu de moyens pour recruter et fidéliser des experts en cybersécurité.** Les petites communes, par exemple, ont de moindres capacités pour se permettre de recruter, étant donné que leur nombre d'agents par habitant est plus faible que celui des grandes, lesquelles peuvent donc se permettre de mieux rémunérer[117].

Le nombre d'agents territoriaux pour 1000 habitants, selon la taille de la commune (en EQTP)



Le nombre d'agents territoriaux par habitant est de 14,4 agents en équivalent temps plein pour 1000 habitants. Ce taux d'administration est plus faible dans les petites communes et plus élevé dans les grandes.

Source : DGCL, Les collectivités territoriales en chiffres, 2021[118]

[117] *Des offres spécifiques de formation apparaissent, dans certaines écoles d'ingénieurs, par exemple.*

[118] https://www.collectivites-locales.gouv.fr/collectivites-locales-chiffres-2021

II.5. RAISON 5 : UN FOISONNEMENT DE SOLUTIONS TECHNIQUES QUI DÉSORIENTE LES NON-INITIÉS

Le domaine de la cybersécurité est vu comme un domaine très technique, d'expert. Faute d'avoir les moyens pour payer un expert et de savoir qui embaucher, les dirigeants de structures abandonnent le sujet et le reportent *sine die*.

Les matériels ou logiciels qui pourraient être recommandés ne présentent pas tous les mêmes niveaux de sécurité, de confiance, de rapport qualité/prix. Des dispositifs de qualification[119] et de certification[120] de l'ANSSI existent, mais ceux-ci concernent les produits (ou des prestataires) au plus haut niveau[121], et non les niveaux de types "intermédiaire" ou "initial".

Un label "ExpertCyber" a également été mis en place par Cybermalveillance.gouv.fr afin d'aider les acteurs à plus facilement identifier des prestataires de cybersécurité (sécurisation, maintenance, assistance à réponse à incident). Il regroupe à date plus de 200 "experts cyber".

II.6. FACTEUR AGGRAVANT 1 : DES ACTEURS PUBLICS AYANT CHACUN COMPÉTENCE POUR INTERVENIR SUR UNE PARTIE DU SPECTRE, AVEC UNE COORDINATION GLOBALE LIMITÉE

L'ANSSI, les CSIRT régionaux, les préfectures, la gendarmerie, la police, la justice, les services de renseignement, Cybermalveillance.gouv.fr : chacun dispose d'une part de compétence dans la coordination, le suivi, l'accueil, l'accompagnement, la réponse à incident ou encore le traitement judiciaire. Chacun dispose de points forts qui pourraient être mieux maillés pour une meilleure compréhension du parcours au profit des entreprises, des collectivités, voire des usagers.

[119] https://www.ssi.gouv.fr/entreprise/qualifications/
[120] https://www.ssi.gouv.fr/entreprise/produits-certifies/
[121] https://www.assemblee-nationale.fr/dyn/15/rapports/due/l15b2415_rapport-information#

Les principaux acteurs de la cybersécurité en France

L'**ANSSI** (Agence nationale de la sécurité des systèmes d'information) est l'agence gouvernementale française chargée de la protection des systèmes d'information de l'État, des opérateurs d'importance vitale et des entreprises stratégiques. Elle assure la veille, la prévention, la détection et la réponse aux cyberattaques, ainsi que la promotion des bonnes pratiques en matière de cybersécurité.

Le **GIP ACYMA** (Groupement d'intérêt public Action contre la cybermalveillance) est une structure regroupant différents acteurs de la cybersécurité en France, tels que l'État, des entreprises, des associations et organisations professionnelles. Le GIP ACYMA opère la plateforme **Cybermalveillance.gouv.fr** qui consiste en un site web destiné à fournir des informations de prévention et une assistance aux particuliers, entreprises, collectivités locales et associations confrontés à un acte de cybermalveillance. La plateforme permet aux utilisateurs de diagnostiquer leurs incidents de sécurité, de disposer de tous les conseils de première intention pour y faire face et le signaler, et d'être mis au besoin en relation avec des prestataires de services spécialisés.

Le **ComCyberGend** (Commandement de la gendarmerie dans le cyberespace) est l'organisme chargé de diriger et de coordonner les activités de la Gendarmerie nationale liées à la lutte contre la cybercriminalité. Le ComCyberGend englobe notamment le C3N (Centre de lutte contre les criminalités numériques).

L'**OCLCTIC** (Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication), service de police spécialisé faisant partie de la Direction centrale de la police judiciaire (DCPJ) chargé de la lutte contre la cybercriminalité.

La **BL2C** (brigade de lutte contre la cybercriminalité), anciennement BEFTI, est une unité spécialisée rattachée à la Préfecture de police de Paris qui se consacre à la lutte contre les atteintes aux systèmes d'information.

La **section J3 du parquet de Paris** regroupe les procureurs qui peuvent, au titre de leur compétence nationale, se saisir des affaires de cybercriminalité complexes, où qu'elles se produisent sur le territoire (les parquets locaux demeurent compétents pour le reste du contentieux).

Les **CSIRT régionaux**, progressivement mis en place à partir de 2022 par la quasi-totalité des différentes régions françaises avec le soutien de l'ANSSI, sont des centres d'alerte et de réaction aux attaques informatiques destinés à traiter les demandes d'assistance des acteurs de taille intermédiaire (PME, ETI, collectivités territoriales et associations) sur leur périmètre et faire l'interface avec les prestataires locaux de réponse à incidents.

Le **Campus Cyber**, situé à la Défense, vise à fédérer la communauté de la cybersécurité et à développer des synergies entre ses différents acteurs : entreprises (grands groupes, PME), services de l'État, organismes de formation, acteurs de la recherche et associations. Le Campus Cyber sera assisté de

déclinaisons régionales (les Campus Cyber régionaux) dans sa mission de structuration de l'écosystème français d'acteurs de la cybersécurité.

Les 10 services de renseignement portent également certaines compétences en la matière, pour les structures qu'ils suivent.

À ces acteurs publics s'ajoutent de nombreux acteurs locaux et territoriaux ainsi que des acteurs privés. Il paraît nécessaire de réfléchir à une manière d'optimiser la mobilisation de toutes ces compétences et prérogatives de manière à étendre le plus rapidement possible la couverture de cybersécurité.

L'organisation de gestion de crise et des chaînes cyber en France, évoquée en annexe 6, illustre combien tous ont à gagner à une coordination étroite et stratégique.

II.7. FACTEUR AGGRAVANT 2 : UN MANQUE DE MATURITÉ DU MARCHÉ DE L'ASSURANCE

La question de l'assurabilité des risques cyber est une question difficile à appréhender. Le contexte des attaques (leur nature, leur volume, leur provenance, leur visée) est mouvant et le modèle économique est complexe à définir. L'étendue de la couverture est très large et la mesure du dommage est extrêmement variable d'un acteur à l'autre, allant du risque réputationnel à la compromission pénale en passant par l'arrêt d'activité.

Selon certains assureurs, le risque cyber serait tout simplement inassurable, plus encore que les catastrophes naturelles, en raison de leur caractère systémique[122], dans la mesure où le risque est permanent, imprévisible et diver-

[122] *https://www.lesechos.fr/finance-marches/banque-assurances/le-risque-cyber-va-devenir-inassurable-selon-le-patron-de-zurich-insurance-1892042#:~:text=Pour%20Mario%20Greco%2C%20le%20directeur,clarifie%20l'indemnisation%20des%20cyberran%C3%A7ons*

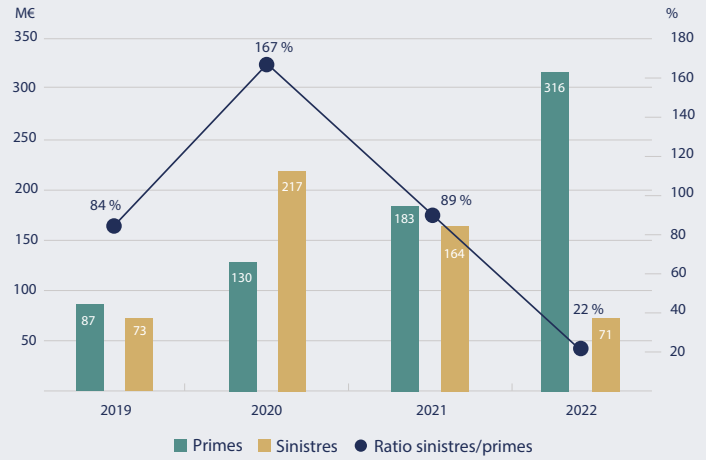
sifié. Les acteurs de l'assurance ont donc encore du mal à adapter leurs modèles pour assurer les petites et moyennes structures contre le risque cyber et ont vécu une année fortement déficitaire en 2020.

Mais **cette croissance globale des attaques a conduit à des primes d'assurance cyber de plus en plus élevées, couvrant de moins en moins de risque.** Ainsi, pour l'ensemble du marché, l'année 2022 fut marquée par une forte augmentation des taux de primes (+54 %) associée à une réduction des capacités (-8 %)[123]. Ces chiffres confirment la tendance observée au cours de l'année 2021 où le volume de primes versées par l'ensemble des entreprises assurées a augmenté de 44 %, alors que les capacités souscrites ont baissé de l'ordre de 20 %[124]. **Certains acteurs estiment payer cher une couverture faible.**

Comme en témoigne le graphique ci-après, ce durcissement des offres a induit une baisse importante du ratio sinistres/primes, toutes entreprises confondues, qui est passé de 167 % en 2020 (signifiant que les sinistres ont coûté 1,6 fois plus aux assureurs que ce qu'ils ont récolté en primes en 2020) à 22 % en 2022[125]. Si en 2021, le marché des grandes entreprises était le seul qui n'était pas déficitaire pour les assureurs, avec un ratio sinistres/primes de 58 % contre 261 % pour les ETI et 325 % pour les petites entreprises, la poursuite du durcissement a permis aux assureurs d'être globalement bénéficiaire (ratios sinistres/primes inférieurs ou égal à 100 %) en 2022[126].

[123] *Rapport LUCY AMRAE 2023*
[124] *Rapport LUCY AMRAE 2022*
[125] *Rapport LUCY AMRAE 2023*
[126] *Rapport LUCY AMRAE 2022*

Le marché français de l'assurance cyber



Source : Rapport LUCY AMRAE 2023

Afin de pouvoir être correctement assurées contre le risque cyber, les petites et moyennes structures doivent avant tout mettre en œuvre les mesures de sécurité minimales, ce qui revient prosaïquement à **"verrouiller la porte avant de prendre une assurance cambriolage".** En effet, le niveau de maturité cyber est généralement insuffisant, et la majorité de ces structures sont en difficulté pour se soumettre à des analyses approfondies, à répondre à de très lourds questionnaires, avant de pouvoir être éventuellement assurées.

La conséquence est que seules les grandes entreprises sont généralement couvertes par une assurance cyber - 94 % des grandes entreprises, 10 % des ETI, 3,5 % des PME en 2022[127].

[127] *Rapport LUCY AMRAE 2023*

La tendance[128] est néanmoins plus favorable en 2022, avec une hausse des entreprises assurées et, comme illustré plus haut, une baisse des primes comme du ratio sinistres/primes. S'agissant des petites et moyennes entreprises, le nombre d'entreprises couvertes reste néanmoins extrêmement faible, et celles qui accèdent à une police d'assurance sont généralement matures, sélectionnées et suivies avec attention.

Ainsi, si le marché de l'assurance cyber semble se stabiliser grâce à l'augmentation de la couverture des entreprises et à la diminution des sinistralités, cette stabilité reste précaire car le montant total des primes collectées en France en 2022 (315M) pour l'assurance cyber équivaut au coût d'un seul événement majeur[129]. **Dès lors, il suffirait d'une seule attaque d'envergure pour compromettre ce fragile équilibre.**

La situation appelle des mesures rapides, qui touchent une large part de l'économie française et de ses collectivités locales. La littérature facilement accessible recèle d'excellentes recommandations pour tout dirigeant cherchant à mieux protéger sa structure. Il faut néanmoins d'abord en être conscient, ensuite être convaincu, enfin savoir par où commencer : identifier les priorités, comprendre vers qui se tourner, prévoir le budget adapté, et embarquer son équipe. Il faut également préparer l'attaque, savoir comment réagir, et vers qui se tourner. Et pour les pouvoirs publics, il s'agit surtout de développer et coordonner la prévention des cyberattaques, mais aussi de traiter au mieux leur remédiation et leur répression.

[128] *Rapport LUCY AMRAE 2023*
[129] *Rapport LUCY AMRAE 2023*

Feuille de route

Ainsi, il apparaît nécessaire de créer les conditions d'un passage à l'échelle pour mobiliser à tous les niveaux et protéger plus exhaustivement le territoire. Cependant, ce nécessaire passage à l'échelle de la part des acteurs locaux publics et économiques est confronté à deux impératifs contradictoires. Face à l'urgence de la situation, le premier plaide pour des mesures d'obligation afin d'accélérer le pas. Au vu du besoin de pédagogie et d'accompagnement d'acteurs qui se sentent démunis, le second plaide pour une approche moins rigide, centrée sur l'incitation.

Le rapport propose ainsi une approche incrémentale.

- Dans un premier temps, il nous a semblé nécessaire de nous concentrer sur ce que les entreprises et collectivités pouvaient faire par elles-mêmes et de les accompagner au plus près dans cette montée en sensibilisation et en protection autonome.

- Dans un deuxième temps, nous pensons que la contrainte réglementaire poussera naturellement ces acteurs à une prise en charge minimale des enjeux de cybersécurité.

- Enfin, une approche plus contraignante pourra être envisagée auprès des plus rétifs afin d'élargir la couverture territoriale et d'assurer un niveau minimum de cybersécurité à l'échelle du pays.

Dans cette démarche de rehaussement collectif du niveau de cybersécurité, l'Institut Montaigne a proposé une méthode simple et rapidement opérationnelle fondée sur les solutions et acteurs existants.

Axe 1

Mobiliser les acteurs en faveur d'un parcours de cybersécurité progressif et simple à même de les protéger et de les préparer aux crises : diagnostic, ambition, précautions, exercices et organisation

Recommandation 1 :

Inciter à recourir à des diagnostics organisationnels et techniques en proposant un référentiel commun comprenant différentes profondeurs de diagnostic

Constat : *Les diagnostics de cybersécurité existants aujourd'hui recouvrent des réalités extrêmement diverses, sont peu normés, insuffisamment réalisés et ne sont pas toujours une garantie suffisante pour le système assurantiel. Les entreprises et collectivités se sentant les moins concernées par la thématique peinent parfois à se situer pour pouvoir prioriser les actions à entreprendre (par où commencer, quelles priorités d'action, vers qui se tourner).*

Afin d'inciter à l'utilisation de diagnostics organisationnels et techniques, il conviendrait d'identifier différents niveaux, regroupés au sein d'un référentiel commun, dont l'ANSSI pourrait avoir la charge en tant que service à compétence nationale. La mise en œuvre de parcours de cybersécurité, à différents niveaux de maturité (cf. annexe 5) pour les entités concernées[130] dans le cadre du Plan de relance, semble avoir particulièrement bien fonctionné.

Ces différents niveaux de diagnostic pourraient être les suivants :

- Un diagnostic initial pourrait se faire en ligne, gratuitement, sur la base d'un auto-diagnostic[131] et d'un scan externe (sur le modèle de ce que propose le NCSC-UK avec un scan externe de vulnérabilités nommé *Early Warning Service*) de ce qui est exposé sur Internet[132]. Ce scan serait effectué par défaut pour les collectivités, et à la demande pour les entreprises intéressées.

- Un diagnostic intermédiaire pourrait être réalisé in situ, en quelques heures. Ce diagnostic serait effectué gratuitement par la puissance publique[133] pour l'ensemble des collectivités[134] ; et effectué, pour la masse des entreprises, par un large écosystème de prestataires (payants, *via* les CCI ou les CSIRT régionaux, pouvant recevoir des subventions nationales, locales ou sectorielles).

- Un diagnostic avancé serait conduit par un écosystème de prestataires certifiés[135] par l'ANSSI, in situ, en quelques jours ; il est parfois subventionné en partie[136], ce qui pourrait être conditionné à l'implémentation des corrections recommandées.
- Un audit serait réalisé sur les systèmes d'information les plus sensibles[137] (ou les plus exposés) de la structure, par un prestataire qualifié par l'ANS-

[131] Tel que proposé par via France Num. Source : https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/evaluez-la-maturite-numerique-de-la

[132] L'ANSSI, par exemple, utilise un outil dénommé IVRE, qui est un "framework open-source" permettant de faire de la reconnaissance de réseaux (scan d'une ou plusieurs adresses IP).

[133] Certains bénéficiaires pourraient avoir le "syndrome du garagiste", et considérer qu'un acteur privé cherchera des failles pour commercialiser des solutions de façon intéressée, tandis que la puissance publique sera par nature désintéressée du point de vue pécuniaire.

[134] Et certaines entreprises, en cas de carence de l'offre privée, en cas d'urgence ou de sensibilité particulière.

[135] Inférieure à la qualification de PASSI (prestataires d'audit de la sécurité des systèmes d'information).

[136] Sur le modèle de ce que pratique Bpifrance (https://www.bpifrance.fr/catalogue-offres/cybersecurite/diag-cybersecurite) pour les entreprises correspondant aux conditions, ou ce que pratiqué l'ANSSI dans le cadre des parcours de cybersécurité faisant suite au Plan de relance, pour les collectivités territoriales répondant aux critères.

SI au niveau PASSI RGS[138]. Cet audit serait potentiellement obligatoire pour toutes les "entités importantes" au sens de la directive NIS 2.

- Un audit de haut niveau serait conduit sur les systèmes d'information critiques[139] de la structure par un prestataire qualifié par l'ANSSI au niveau PASSI LPM[140]. Cet audit serait potentiellement obligatoire pour toutes les "entités essentielles" au sens de la directive NIS 2.

Le résultat du diagnostic fournira à une entreprise (ou collectivité) une liste des critères manquants pour prétendre au niveau de cybersécurité adéquat pour la structure (cf. recommandation 2). La mobilisation sera ainsi adaptée, et la structure ayant pris conscience des risques sera en mesure de prioriser ses investissements en se focalisant sur les critères restant à atteindre.

La standardisation des diagnostics facilitera la comparaison des résultats et permettra une meilleure évaluation de l'efficacité des mesures de cybersécurité mises en place post-diagnostic.

[137] Les systèmes d'information moins sensibles devant faire l'objet d'un diagnostic du niveau "argent" au minimum.

[138] Un PASSI RGS (Prestataire d'Activités de Sécurité et de Services d'Infrastructure Réseaux et Systèmes) est un label de qualification à destination des prestataires de services et d'audits informatiques, délivré en France dans le cadre du Référentiel Général de Sécurité (RGS), un ensemble de règles, de recommandations et de bonnes pratiques en matière de sécurité des systèmes d'information, établi par l'ANSSI en collaboration avec d'autres organismes.

[139] Les systèmes d'information non critiques devant faire l'objet d'un diagnostic du niveau "argent" au minimum.

[140] Le PASSI LPM (Prestataire d'Activités de Sécurité et de Services d'Infrastructure Réseaux et Systèmes pour les besoins de la LPM) est un label de qualification délivré en France dans le cadre de la Loi de programmation militaire (LPM), spécifiquement destiné aux prestataires de services et d'audits qui souhaitent travailler avec des organismes relevant du domaine de la défense et de la sécurité nationale.

Les principaux acteurs de la cybersécurité en France

Di@GoNal[141] est un dispositif de diagnostic proposé par la Gendarmerie nationale, dans la continuité de l'auto-diagnostic "Immunité Cyber". D'une durée de 2h environ, il est réalisé sur place par un gendarme spécialisé, les résultats sont confidentiels. Le diagnostic est évoqué plus longuement dans ce rapport au titre d'une étude spécifique sur le terrain.

MonAideCyber, en cours de développement au sein de "beta.gouv.fr", l'incubateur de services publics numériques du gouvernement, est un futur service gratuit de diagnostic cyber rapide mis en place en France pour aider les entités publiques et privées à renforcer leur cybersécurité. Les diagnostics seront effectués par des tiers de confiance (acteurs locaux publics et associatifs déjà engagés dans la sécurisation des entités publiques et privées) qui seront formés et outillés par l'ANSSI par l'intermédiaire d'une plateforme dédiée. Ces diagnostics permettront d'établir un état des lieux de la maturité cyber de l'entité, d'identifier les lacunes et de proposer des actions concrètes à fort impact. Le dispositif Di@GoNal aurait vocation, à terme, à être intégré dans MonAideCyber.

Diag Cybersécurité est un diagnostic numérique lancé par Bpifrance a lancé en mars 2023 pour aider les TPE/PME à mieux se protéger face aux menaces cyber, d'un coût de 2200€ par site subventionné à hauteur de 50 %. Ce diagnostic, d'une durée de 4 jours, est réalisé par des consultants/auditeurs spécialisés et comprend quatre étapes : un pré-cadrage téléphonique, une visite sur site (pour évaluer le niveau de sécurité

[141] Diagnostic opérationnel national.

numérique des infrastructures), une évaluation du niveau de maturité cyber et enfin une restitution comprenant un état des lieux et un plan d'action adapté à l'entreprise.

L'État conforte à ce stade, dans sa planification[142], la piste d'un auto-diagnostic gratuit, la poursuite des parcours de cybersécurité pour certaines collectivités, et l'extension de cette approche aux entreprises dans un "bouclier cyber".

[142] *Annonce du ministre du numérique le 16 novembre 2022.*

Recommandation 2 :

Fixer une cible de cybersécurité à atteindre pour les structures, en fonction de leur criticité et de leurs moyens, et les inciter à progresser dans la durée en proposant un système de badges les aidant à prioriser leurs arbitrages

Constat : *les entreprises et collectivités ont parfois peu d'incitations à s'améliorer. La chaîne de valeur est parfois fragilisée par un manque d'informations fiables sur le niveau de sécurité numérique des autres structures[143], ce que le diagnostic proposé en Recommandation 1 permettra d'améliorer.*

[143] *Client, fournisseur, concurrent...*

Il existe un intérêt à inciter des acteurs les moins préparés à débuter une démarche simple, adaptée et incrémentale. La mise en place de standards communs de cybersécurité constitue une piste[144] des pouvoirs publics. Le levier réputationnel permettrait une identification du niveau de chaque structure par tout un chacun (personnels, citoyens, clients, prestataires, fournisseurs, sous-traitants...). Ainsi, à chaque niveau de maturité cyber correspondrait un badge. Ce système de badges permettrait aux structures de prioriser leurs investissements en cybersécurité. Par exemple :

- une grande entreprise labellisée "argent" pourrait favoriser le choix de ses sous-traitants sur la base de leur niveau de protection (dans une logique équivalente à celle des normes ISO), afin de limiter les risques d'une attaque par chaîne d'approvisionnement ou d'une attaque par latéralisation pouvant résulter des interconnexions entre systèmes d'information ;
- les badges pourraient être des niveaux pris en compte dans les appels d'offres[145] d'une collectivité.

Une telle approche permettrait aux parties prenantes de progresser dans le temps, à leur rythme, en fonction de l'importance de la situation et de leurs moyens. La démarche permettrait également de **simplifier et rationaliser, notamment pour les banques et les assurances, le processus de "notation des risques"** inhérent à la souscription d'un prêt ou d'une police d'assurance[146].

Considérant la fluidité du marché intérieur et de l'espace européen, et pour éviter tout risque d'accusation de protectionnisme, il pourrait être cohérent et utile que la même logique puisse être induite à l'échelle européenne. Les deux exemples européens les plus pertinents sont ceux déployés en Belgique et au Royaume-Uni.

[144] *https://www.tresor.economie.gouv.fr/Articles/2022/09/07/remise-du-rapport-sur-le-developpement-de-l-assurance-du-risque-cyber*

[145] *En fonction du cadre juridique de marchés publics applicable.*

[146] *En complétant les analyses effectuées par les agences spécialisées dans le "cyber rating" dont les algorithmes peuvent manquer de transparence et dont les notes sont difficilement comparables d'une agence à l'autre : https://www.usine-digitale.fr/article/jusqu-ou-le-cyber-rating-peut-il-s-imposer-dans-l-assurance-cyber.N2118671*

Au Royaume-Uni, le NCSC-UK a lancé un système de labellisation Cyber Essentials qui fournit des conseils et une assistance aux petites et moyennes entreprises pour améliorer leur posture de cybersécurité. Les entreprises peuvent obtenir[147] une certification Cyber Essentials prouvant qu'elles ont mis en place des mesures de sécurité de base pour se protéger contre les cyberattaques courantes. Pour sa part, la Belgique identifie 4 niveaux de maturité[148] pour la cybersécurité des entreprises, dans son schéma *Cyberfundamentals.*

La logique incitative présente de nombreux avantages dans un contexte de tension dans les métiers du numérique est forte, la situation économique n'est pas toujours favorable à de lourds investissements, et le niveau de maturité initial des structures ciblées est souvent trop faible. L'incitation pourrait être remplacée par l'obligation à terme (quelques années après la mise en place du système incitatif, par exemple), pour laisser aux structures et au marché le temps de s'organiser, tout en soulignant l'intérêt à agir.

Le tableau présenté ci-dessous propose une logique à 5 niveaux de maturité dans la sécurisation des acteurs. Le niveau terminal, appelé "Platine", correspond à la cible à atteindre pour les OIV et les OSE. S'agissant d'obligations légales et réglementaires qui leur sont propres, il n'est pas utile de les détailler; même une structure qui ne serait pas d'importance vitale peut néanmoins se fixer elle-même l'ambition d'atteindre ce niveau de maturité. Pour se prévaloir de l'un des 4 autres niveaux de maturité (de "Graphite" à "Or"), une liste de critères est proposée, permettant d'obtenir le badge afférent. Ces critères s'appuient, pour une grande partie d'entre eux, sur les 23 règles de sécurité (listées à l'annexe 4) que doivent mettre en œuvre les opérateurs de services essentiels (OSE) dans le cadre de l'application de la directive NIS.

Le tableau représente l'organisation-type qu'il serait utile d'atteindre, sans prétendre être exhaustive. Une version détaillée du tableau (précisions des briques de sécurité recommandées) est présentée à l'annexe 6 du rapport. En outre, ce tableau constitue une approche globale fondée sur une corrélation entre la taille de l'entité et le niveau de badge. Il existe évidemment des entités stratégiques pour lesquelles le niveau adéquat sera supérieur à celui correspondant aux autres entités de la même taille[149]. Le principe de Pareto en constitue l'essence, avec un coût d'entrée modéré et un encouragement à faire progressivement mieux. Enfin, il est important de noter que même une structure parvenue à l'issue de la démarche (Platine) n'en est pas pour autant immunisée : la menace demeure prégnante et évolutive, mais la structure aura démontré avoir entrepris tout ce qui était raisonnable pour s'en protéger.

Critères / Badges	Graphite	Bronze	Argent	Or	Platine (OIV/OSE)
Qui suis-je (entité type)	TPE (PME < 10 salariés) Très petite collectivité (-1000 hab) ~ 1 000 000	PME entre 10 et 50 salariés Petite collectivité (1000 à 5000 hab, syndicats mixtes) ~ 150 000	ETI et PME > 50 (hors NIS 2) Moyenne collectivité (+5000 hab, EPCI) ~ 35 000	"Entités importantes" NIS 2 Grande collectivité ~ 10 000	OIV + OSE NIS ("entités essentielles" NIS 2) ~ 700
Je connais mes vulnérabilités (diagnostic / audit)	Autoévaluation En ligne avec scan externe	In situ 2h Gratuit, ou prestataire labellisé	In situ 4 jours Prestataire certifié (2000€)	Audit PASSI RGS	Audit PASSI LPM

[147] *Environ 6 % des entreprises britanniques étaient certifiées Cyber Essentials en 2022, et 1 % étaient certifiées Cyber Essentials Plus.*

[148] *https://ccb.belgium.be/fr/cyberfundamentals-framework*

[149] *Par exemple, une PME de 20 salariés ayant des contrats avec le secteur régalien pour des prestations sensibles peut très bien chercher à atteindre le niveau "Or". De même, une PME de 70 personnes spécialisée dans le service à la personne à domicile pourrait se contenter d'un niveau "Bronze".*

[150] *Au total, la France compte environ 1 million d'entreprises avec au moins un employé, 45 000 collectivités locales (avec et sans fiscalité propre) et 3 000 établissements de santé.*

[151] *https://www.cybermalveillance.gouv.fr/tous-nos-contenus/label-expertcyber/decouvrir-le-label-expertcyber#h-1-qu-est-ce-que-le-label-expertcyber*

Critères / Badges	Graphite	Bronze	Argent	Or	Platine (OIV/OSE)
Je me forme et m'entoure (compétences numériques de gouvernance)	Sensibilisation dirigeant 2h ACYMA	Conseiller (CSN) + MOOC SecNum académie	MOOC + CSN + RSSI temps partagé	MOOC + CSN + RSSI temps plein	N/A
J'acculture mon équipe (procédure de gestion d'attaque)	Alerte "incendie" cyber	Exercice de simulation d'attaque simple	Exercice avancé (PCA/PRA partiel)	Exercice de crise (PCA/PRA complet)	Homologuée
J'anticipe l'interruption d'activité (provision pour risque cyber / garanties offertes par la police d'assurance)	Préparation et diffusion d'une liste de bonnes pratiques à la suite de l'alerte incendie cyber	Provision pour risque cyber (2 % du chiffre d'affaires annuel)	Assurance gestion de crise (versements rapides forfaitaires)	Assurance gestion de crise + RC cyber de l'entreprise et du dirigeant	Obligations spécifiques OIV/OSE
Je fais appel à des professionnels formés/vérifiés	Tout professionnel	Labellisés Expert Cyber[151]	Certifiés ANSSI	Qualifiés ANSSI	
J'organise mes sauvegardes et mes données	+	+	++	++	
Je protège les points d'entrée de mon SI	+	+	++	+++	
Je sécurise mes données et applications	+	+	++	+++	
Je protège les postes de mon SI	+	++	+++	++++	
Je sécurise le réseau de mon SI	+	++	+++	+++++	
Je centralise et supervise mon SI pour mieux détecter et traiter les menaces	+	++	+++	+++++++	
Quelle durée de validité	1 an	2 ans	2 ans	3 ans	3 ans

Le coût moyen des différentes briques de sécurité

Il est intéressant de disposer d'ordres de grandeur[152] du coût des principaux outils et services pouvant utilement être déployés (coût moyen constaté annuel et par poste) :

- solutions intégrées de sécurité (services managés[153]) : 135 € ;
- coffre-fort numérique : 9 €;
- sauvegarde sécurisée : 40 €.

Au total, dans une petite structure, le coût annuel peut représenter 200 à 300 €/an/poste.

Les niveaux Argent et Or requièrent de souscrire à une police d'assurance offrant des garanties spécifiques. L'offre assurantielle pour les acteurs ciblés dans ce rapport n'est pas pleinement mature pour passer à l'échelle, à date (cf. section II.7 de notre état des lieux). Une uniformisation des outils de diagnostic (recommandation 1) et une élévation collective du niveau de maturité par l'incitation (recommandation 2) sont des prérequis à une généralisation de l'assurance cyber, qui présente de nombreux avantages. Dans l'attente, la nécessité d'une assurance cyber pour obtenir un badge de cybersécurité est ainsi réservée aux niveaux les plus avancés.

[152] *Les coûts peuvent varier fortement selon le format de la structure (dégressivité), le niveau d'intéressement du tiers (offre privée ou subventionnée) et le caractère isolé ou mutualisé de l'offre.*

[153] *Patches automatiques dont antivirus nouvelle génération (EDR), protection des réseaux (firewall), détection de vulnérabilités et sécurisation des annuaires (avec l'ANSSI), sensibilisation au phishing (campagnes de faux mails), analyse de courriels douteux, sensibilisation et formation.*

Pour obtenir le badge de cybersécurité (et la faire évoluer), une déclaration en ligne dans un registre national dédié assure souplesse et traçabilité[154].

Une fois le diagnostic établi et les briques de sécurité manquantes installées, le responsable de la structure procède à la déclaration de maturité cyber. Les réponses apportées aux différents critères (par menus déroulants, et versement éventuel de preuves numériques), permettent au système d'attribuer le niveau de badge atteint (graphite, bronze, argent, or ou platine) et sa durée de validité, sur la plateforme unique de signalement des faits cyber (recommandation 8). Dans l'hypothèse d'installations sur plusieurs sites, les niveaux déclarés devraient correspondre soit à la situation homogène, soit à l'installation la moins sécurisée de l'ensemble de l'entreprise ou de la collectivité (principe du maillon faible). Pour autant, la démarche entreprise et le badge obtenu ne sont pas des garanties d'immunité face à une attaque; mais le fait d'être mieux sécurisé qu'un voisin peut suffire à éviter de devenir une victime.

L'annonce du ministre du numérique (le 16 novembre 2022), d'une plateforme mutualisée de services sécurisés pour un nom de domaine, une messagerie puis l'hébergement de données, propose d'apporter un niveau élevé de sécurité aux utilisateurs qui pourront s'en prévaloir. Le recours à ces solutions, dont la sécurité est garantie par la puissance publique, devrait permettre d'atteindre au minimum le niveau Argent, en fonction des services utilisés et des spécifications techniques. D'une façon générale, les plus petits acteurs ont tout intérêt à se tourner vers le *cloud* de confiance[155].

[154] *En cas de cyberattaque ou d'incident de sécurité, les entreprises seraient invitées à le notifier sur plateforme unique, et bénéficient alors d'une absence de "double sanction" : en cas de contrôle ou d'enquête judiciaire faisant suite au signalement, l'éventuelle faille par laquelle l'attaque se serait produite ne serait pas reprochée à la structure, sauf négligence lourde. Il s'agit ici de limiter le risque de fausse déclaration (délit) dans l'obtention des badges de cybersécurité.*

[155] *Infonuagique de confiance (dans les documents officiels).*

Recommandation 3 :

Limiter nativement la présence de vulnérabilités et de failles dans les produits et équipements numériques disponibles sur le marché européen en exploitant tout le potentiel du règlement européen *Cyber Resilience Act*, et informer les utilisateurs en temps réel en cas de trafic Internet suspect grâce à une "cyber vigie" opérée par les opérateurs de télécommunications

Constat : *les éditeurs numériques commercialisent parfois des produits insuffisamment sécurisés ou peu maintenus, avec un risque faible d'engagement de leur responsabilité civile en cas d'attaque - du fait de la complexité des systèmes, des attaques elles-mêmes et de l'imbrication des produits. Les opérateurs de télécommunication, quant à eux, maîtrisent en partie (hors flux chiffrés) les données transitant sur leurs réseaux, et pourraient informer l'utilisateur des risques de son trafic. Il s'agit donc de proposer des solutions transparentes pour l'utilisateur en responsabilisant en amont de la chaîne numérique.*

> ***En s'inscrivant dans la dynamique de "sécurisation systémique" que va permettre le Cyber Resilience Act pour mettre à contribution les opérateurs de télécommunications et les fournisseurs d'accès à Internet (cf. encadré sur le Cyber Resilience Act)***

Le projet de règlement européen *Cyber Resilience Act*, présenté le 15 septembre 2022 par la Commission européenne, vise à renforcer la cybersécurité au sein des États-membres de l'Union en obligeant les fournisseurs et les fa-

bricants de produits numériques, qu'ils soient matériels ou logiciels, à inclure par défaut - "*by design*" - des modules de sécurité (authentification multi-facteurs, etc.) et à limiter la présence de vulnérabilités tout au long du cycle de vie du produit (de sa conception jusqu'à son retrait du marché en passant par sa commercialisation).

De manière analogue aux objectifs énoncés par la récente stratégie américaine de cybersécurité publiée en mars 2023[156], le CRA proposera un modèle d'engagement de la responsabilité civile des fabricants et des éditeurs dont le produit numérique ou le logiciel aurait présenté une vulnérabilité flagrante à l'origine d'une campagne de cyberattaques[157].Un tel dispositif législatif soutiendra donc la maturité de l'écosystème de l'assurance en favorisant l'articulation des chaînes de responsabilités.

Le règlement, directement applicable en droit interne (sans transposition), est toujours en cours de rédaction, et offre ainsi toutes les chances d'une norme européenne faisant référence, à même de contraindre jusqu'aux plus grands acteurs[158] à une prise en compte complète. Dans cette perspective, et comme c'est le cas dans d'autres domaines (dans l'aéronautique, par exemple), un éditeur qui aura manqué à son obligation de moyens et d'information relativement au niveau initial et continu de la sécurité de ses produits, pourrait davantage craindre l'engagement de sa responsabilité, et les conséquences financières attachées.

> ***Par une "cybervigie", levant une alerte en temps réel en cas de trafic Internet suspect grâce aux opérateurs de télécommunications***

[157] *"We must [...] reshape laws that govern liability for data losses and harm caused by cybersecurity errors, software vulnerabilities, and other risks created by software and digital technologies".*

[156] *"Where such a lack of safety consists in a lack of security updates after placing the product on the market, and this causes damage, the liability of the manufacturer could be triggered. Obligations for manufacturers that concern the provision of such security updates should be laid down in this Regulation" https://ec.europa.eu/newsroom/dae/redirection/document/89543*

[158] *L'échelon européen est déterminant pour agir, dans la mesure où de nombreux produits sont américains ou asiatiques.*

La dynamique volontariste de cybersécurité par défaut du futur *Cyber Resilience Act* pourrait conduire les opérateurs de télécommunications et les Fournisseurs d'Accès à Internet (FAI) à embarquer des fonctionnalités de sécurité dans les différents équipements déployés sur leurs réseaux, notamment les routeurs et autres boxs Internet déployés chez les "petits" comptes tels que les particuliers ou les petites entreprises.

Ainsi, en matière de "détection *a posteriori*", ces équipements pourraient devenir "proactifs" et augmenter de manière systémique la sécurité des réseaux nationaux en embarquant un système de levée d'alerte en cas de détection de trafic TCP/IP malveillant au niveau des routeurs et des box Internet.

Aujourd'hui, bien que les opérateurs de télécommunications aient déjà des obligations en matière de surveillance du trafic, celles-ci concernent principalement le cœur du réseau et servent uniquement à l'État pour des enjeux de sécurité nationale[159]. Même si le trafic est généralement chiffré de bout-en-bout aujourd'hui (notamment avec des protocoles type HTTPS), de nombreuses possibilités techniques demeurent pour permettre, *a minima*, une supervision dudit trafic *via* les résolutions DNS[160].

Dès lors, il serait possible pour les opérateurs et les fournisseurs d'accès à Internet de mettre en place une supervision au niveau "local" levant automatiquement une alerte en cas de communication avec des adresses IP ou des domaines vus par des bases de scan en ligne comme cherchant à exploiter des vulnérabilités majeures connues ou correspondant à des serveurs de commande & contrôle (C2) associés à des codes malveillants génériques (type Cobalt Strike ou autre). Les opérateurs pourraient ainsi se prévaloir, auprès de leurs clients et dans la présentation de leurs offres, d'un niveau de sécurité plus élevé relativement au risque de cyberattaque.

[159] *Par exemple, l'article 34-1 de la LPM 2019-2025 permet de forcer l'opérateur à rechercher des marqueurs de compromission sur son réseau.*

[160] *Souvent en clair et utilisant le résolveur DNS de l'opérateur. Et les "netflows" associées (connexions HTTP consécutives qui font apparaître en clair les IP source et destination - sauf en cas d'utilisation d'un tunnel VPN chiffré).*

Les alertes éventuelles seraient remontées à l'administrateur local *via* une notification dans l'espace d'administration du routeur/box Internet, voire d'un *popup* sur le bureau de l'ordinateur de ce dernier (un logiciel client spécifique serait alors nécessaire). C'est l'administrateur qui prendrait alors la décision de bloquer (temporairement) ou non le trafic potentiellement malveillant (lié à une adresse IP ou un nom de domaine) associé à l'alerte.

Un système analogue[161] a déjà été mis en place à partir de 2018 au Royaume-Uni par le NCSC-UK. Nommé "*Threat-o-matic*"[162] ; l'outil fut conçu à la base pour identifier les adresses IP à l'origine d'attaques DDoS ciblant des entités britanniques et alerter rapidement les fournisseurs d'accès pour que ceux-ci mettent ces adresses IP en blocage. Le périmètre de l'outil aurait été étendu pour permettre de relayer n'importe quel type d'indicateur de compromission associé à un mode opératoire et en demander le blocage aux fournisseurs d'accès à Internet.

En outre, à des fins de "détection *a priori*", les routeurs et les box Internet pourraient également embarquer un dispositif de type sonde qui identifiera automatiquement les vulnérabilités des équipements connectés au réseau interne (qui pourraient être exploitées par des attaquants potentiels) et préviendra par courriel le titulaire du contrat Internet correspondant. Les opérateurs pourraient potentiellement s'associer à des *start-ups*[163] développant déjà ce type de services pour le proposer à leurs clients, qui présente un intérêt majeur pour sécuriser les très nombreux objets connectés aux box, souvent bien peu sûrs.

Cette "cyber vigie" pourrait elle aussi constituer une incitation réputationnelle des opérateurs pratiquant ces niveaux sommitaux de détection et d'information sur les flux de leurs clients, pour en faire un emblème de sécurité numérique[164]. Si elle ne semble pas poser de défi technique pour être réalisée, la question du consentement à payer ce type de services peut être un frein. Le cadre légal, quant à lui, se prêtera plus facilement à une mise en place au profit des personnes morales que des personnes physiques.

[161] *Mais fonctionnant au niveau backbone (cœur de réseau) et non au niveau des équipements périphériques et implémentant un blocage et non un simple avertissement.*

[162] *https://www.zdnet.fr/actualites/ncsc-mon-travail-ce-n-est-pas-de-mettre-fin-au-cybercrime-c-est-de-l-envoyer-en-france-39874973.html*

[163] *Telles que ProHacKtive et sa solution Sherlock.*

Recommandation 4 :

Exhorter les entreprises et collectivités à considérer le risque cyber comme une préoccupation stratégique encadrant les choix humains, organisationnels, budgétaires et techniques de leur activité

Constat : *les conséquences d'une cyberattaque peuvent être très graves, allant de la perte de données sensibles à la perturbation des activités, voire à leur arrêt complet. Les leviers permettant de les éviter, loin d'être purement techniques, concernent tout aussi bien la stratégie de l'entité, son organisation, son personnel et le budget consacré à la question. Autant de points maîtrisés par la gouvernance de la structure.*

Pour minimiser ces risques, que ce soit en matière de probabilité d'occurrence ou d'impact, il est essentiel de **faire de la cybersécurité une préoccupation stratégique des dirigeants** et de relayer celle-ci par l'intermédiaire de mesures opérationnelles. La simplification de la vie administrative des entreprises étant une politique prioritaire du gouvernement, ce dispositif est évoqué comme une incitation (dans le système de badges) plutôt que comme une obligation.

[164] *La démarche est différente du projet de "filtre anti-arnaque" (projet de loi n°593 du 10 mai 2023 "Sécuriser et réguler l'espace numérique"), qui s'attache à sécuriser la navigation internet des particuliers pour éviter le hameçonnage.*

Par ailleurs, des témoignages de dirigeants qui ont dû faire face à une cyberattaque au cours de l'année écoulée pourraient partager leur expérience vers leurs pairs. En effet, ces discours sont généralement les plus mobilisateurs (en particulier dans un même secteur d'activité, ou entre des structures de physionomie comparable). Ces partages d'expérience existent souvent de façon informelle, et gagneraient à être systématisés. Ainsi durant le "Mois européen de la Cybersécurité" (calé en octobre), des retours d'expérience (RETEX) entre dirigeants de TPE/PME/ETI pourraient être organisés *via* les fédérations professionnelles ou les centres régionaux de réponses à incidents.

La souscription à une police d'assurance cyber correspond à un niveau élevé de prise en compte du risque. En effet, l'assureur vérifie systématiquement le niveau de maturité de la structure avant de passer à la phase contractuelle; puis, son intérêt est d'éviter la réalisation du risque, et d'en limiter les effets en cas de réalisation. Autant d'éléments qui concourent à une amélioration permanente de la prise en compte du risque cyber. Si les offres centrées sur la remédiation, voire sur la couverture de responsabilité civile, semblent fonctionner, il en va différemment des contrats couvrant les pertes d'exploitation. L'assurance cyber ne peut donc concerner, dans un premier temps[165], que les structures ayant une maturité au moins intermédiaire. Pour démontrer la prise en compte du risque cyber dans un maximum d'entreprises, la mention de ce risque dans le rapport de gestion (faisant partie des documents sociaux qui incluent également l'inventaire et les comptes annuels), préparé en amont de chaque assemblée générale ordinaire, pourrait être vérifiée par l'expert-comptable (si applicable) et validée par le commissaire aux comptes[166] (si applicable).

Une possibilité complémentaire consisterait à **inciter l'expert-comptable**

[165] *La création d'un système d'indemnisation à plusieurs niveaux (modèle de la nouvelle "assurance récolte" de 2023, à 3 niveaux) est également intéressante, ou la création d'un fonds de garantie contre les cyberattaques. Dans les deux cas, pour fonctionner, une élévation du niveau général de cybersécurité est un préalable.*

[166] *Un tel dispositif est forcément réservé aux niveaux élevés du système de badges, dans la mesure où une partie seulement des acteurs considérés sont formés aux risques cyber.*

à recommander au dirigeant, si nécessaire et en l'absence d'une police d'assurance couvrant le risque cyber, la prise d'une provision pour risque (qui serait non déductible du bénéfice imposable) au passif des entreprises qui n'auraient pas suffisamment couvert la question, si leur situation le permet. Si l'on considère une moyenne d'interruption d'activité de 16 jours en cas de cyberattaque, la provision pourrait être fixée à 4 %[167]. Un tel niveau peut paraître très élevé pour beaucoup de structures, et un niveau plus faible (2 % par exemple) pourrait suffire à couvrir au minimum les frais de remédiation, pour reprendre l'activité au plus vite. Cette provision aurait vocation à être validée par le commissaire aux comptes. Cette solution aurait pour avantage de n'avoir d'effet que sur le seul plan comptable, en réduisant le bénéfice distribuable[168]. Dans le système de badges, cette provision se substitue à la piste d'une assurance cyber pour les niveaux intermédiaires, considérant le temps nécessaire au système assurantiel pour continuer à se développer en direction des acteurs les moins préparés au risque cyber. Une fois le secteur assurantiel suffisamment mûr, la provision, qui remplit la même fonction de préservation devant la réalisation d'un risque, pourra être supprimée[169].

Pour les collectivités locales, il s'agira d'instaurer un schéma local des risques cyber, décliné dans chaque collectivité, sur le modèle du plan communal de sauvegarde[170], une cyberattaque étant en un sens une calamité majeure pour une collectivité. Ce schéma devrait évoquer la gestion de crise, la continuité et reprise d'activité, et être suivi par la préfecture au sein d'un état-major cyber dédié[168]. Dans le système de badges, l'existence d'un schéma local des risques cyber constitue un critère à partir du niveau "bronze" pour les collectivités locales.

En résumé, il s'agit ici de **sensibiliser les dirigeants des petites entreprises**

[167] *Selon Emsisoft, les compromissions par rançongiciels entraînent un arrêt d'activité pendant 16 jours en moyenne : https://www.emsisoft.com/en/blog/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis/ (16/365 = ~4 %)*

[168] *Donc, a fortiori, la marge de manœuvre pour verser des dividendes, pour les entreprises le pouvant.*

[169] *Elle n'a pas pour finalité d'encourager les acteurs à s'auto-assurer.*

[170] *Défini à l'article L731-3 du Code de la sécurité intérieure.*

[168] *Au sens du Livre blanc sur la sécurité intérieure (2020), les préfectures doivent organiser un "état-major cyber".*

et des collectivités aux risques majeurs liés aux cyberattaques pour qu'ils en perçoivent les enjeux stratégiques sous-jacents, ceci afin de les inciter à faire les choix organisationnels, budgétaires et humains adéquats pour protéger efficacement leur organisation.

C'est le sens de **l'expérimentation de terrain conduite dans le Calvados** (ainsi que dans deux entreprises de l'Eure) au cours des derniers mois. **130 communes (sur 528), 10 entreprises et 6 hôpitaux ont pu ainsi être diagnostiqués par la Gendarmerie nationale**, en utilisant son outil Di@GoNal.

En effet, la Gendarmerie nationale a développé un outil de diagnostic gratuit conçu pour les collectivités locales puis étendu aux entreprises et établissements de santé. Ce diagnostic permet de délivrer une évaluation au plus près des acteurs, sur place, mais aussi des conseils très concrets afin de mieux circonscrire les vulnérabilités dont ils n'ont parfois pas conscience[172]. Il repose sur une auto-évaluation réalisée par le responsable de la structure visitée (d'une durée de 30 minutes), un diagnostic déclaratif mais guidé, *in situ*, conduit par un gendarme spécialisé (d'une durée de 2 heures) puis la rédaction d'un rapport de synthèse et de recommandations effectuée par la gendarmerie au bénéfice de la structure. Un exemple de la synthèse des évaluations conduites (thèmes et cotation des maturités et des risques) figure en annexe 7.

Cette démarche, encore peu connue, a été réalisée d'abord par des personnels spécifiquement formés dans les unités territoriales du groupement, puis par un personnel spécialisé au groupement, **en lien avec les chambres consulaires départementales et certaines fédérations professionnelles.**

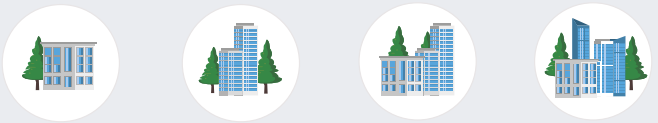
A date, le bilan des structures diagnostiquées par la Gendarmerie nationale avec cette méthode est le suivant :

[172] *En premier lieu, les rappels de bonnes pratiques numériques (force des mots de passe, protection du Wifi, séparation des usagers professionnels et privés…); en second lieu, l'importance d'être avisé d'une attaque en cours et d'y réagir très vite (par exemple : prévoir un bouton d'arrêt d'urgence des connexions internet, activable sur place par un agent de sécurité en heures non-ouvrées sur ordre du responsable de la sécurité numérique).*

1034 collectivités dont 22 ultramarines

40 % n'ont pas de délégué à la protection des données
54 % déclarent ne pas avoir de référent cybersécurité
74 % n'ont pas de plan de gestion de crise cyber

46 entreprises dont 2 ultramarines



61 % n'ont pas de délégué à la protection des données
56 % déclarent ne pas avoir de référent cybersécurité
71 % n'ont pas de plan de gestion de crise cyber

33 établissements

7 % n'ont pas de délégué à la protection des données
0 % déclarent ne pas avoir de référent cybersécurité
13 % n'ont pas de plan de gestion de crise cyber

Ce bilan révèle également qu'au niveau territorial, **1 collectivité sur 10 (la plus petite ayant 200 habitants), 1 entreprise sur 4 et 1 établissement de santé sur 5 ont déjà été victimes d'un rançongiciel.** 28 % des collectivités, 60 % des entreprises et 56 % des établissements de santé ont été victimes de cybermenaces.

Il en ressort que les entreprises sont généralement les plus conscientes du risque, les plus convaincues de l'intérêt d'agir et, paradoxalement, les moins demandeuses d'un regard des services de l'État sur la question. Dans les structures publiques, la tendance constatée est que plus elles sont petites, plus les leviers sont faibles et plus la vulnérabilité est grande.

Un gros travail de sensibilisation des collectivités est donc nécessaire. **L'idée est de proposer une acculturation à la lutte contre les cybermenaces.**

Dispensée sur trois heures, la sensibilisation locale permet à un maximum d'employés (et non plus seulement au responsable) de saisir les éléments essentiels des domaines suivants :

- les principales menaces et leurs conséquences : attaques par rançongiciels, par messagerie électronique (et pièces jointes infectées), la redirection de site, la dissimulation, l'usurpation du nom de domaine ;
- les solutions simples (les sauvegardes, la gestion des autorisations, les droits utilisateurs, la prévention) et les bonnes pratiques ;
- le dépôt de plainte ainsi que le signalement sur les différents sites dédiés.

Initialement réalisées dans les locaux de la gendarmerie[173], ces séances de sensibilisation sont désormais réalisées directement dans les structures elles-mêmes (pour autant que le volume de personnel à former soit suffisant).

Des éléments pratiques ont permis d'affiner la démarche :

[173] *Brigade, compagnie, groupement selon les capacités d'accueil.*

- les personnels sont plus réceptifs face à un formateur se déplaçant sur leur site, plutôt que si eux-mêmes doivent se déplacer (ou si cela est fait à distance, ou en visionnant un média sans interaction) ;
- ces échanges font évoluer les mentalités et facilitent la tâche de la gouvernance et du responsable de la sécurité numérique (leur crédit est supérieur lorsqu'ils sont appuyés dans la structure par un discours analogue d'un agent de l'État) ;
- une méfiance peut subsister chez certains face au démarchage de nombreux acteurs privés qui proposent également ce type de sensibilisation ("que va-t-il essayer de me vendre?"). Dans ce cas-là, et même si le marché a toute sa place et une utilité indéniable, pour les acteurs les moins informés, il est préférable de se tourner vers les acteurs publics et de réserver le peu de moyens parfois disponibles à l'amélioration des solutions numériques elles-mêmes.

L'analyse conduite en partenariat avec le ComCyberGend et l'Institut Montaigne, sur le Calvados, illustre la pertinence de cette démarche d'acculturation.

Au 1er juin 2023, quatre types de publics ont ainsi été approchés :

- collectivités locales : 37 séances de sensibilisation pour 530 personnes formées ;
- TPE/PME : 3 séances de sensibilisations pour 107 personnes formées ;
- hôpitaux : 9 séances de sensibilisations pour 186 personnes formées ;
- les élèves du Service national universel ont également été formés.

Comme indiqué ci-dessus, cette démarche a été réalisée par des personnels du groupement de gendarmerie départementale spécialement formés, en lien avec la préfecture et la délégation régionale de l'ANSSI.

L'Institut Montaigne, en lien avec le Mouvement des entreprises de taille intermédiaire (METI) et la Gendarmerie, sur la base très concrète de cette

expérience, a ainsi pu affiner en temps réel la validité de certaines des recommandations du présent rapport.

Recommandation 5 :

Organiser une simulation annuelle d'alerte cyber (équivalent de "l'alerte incendie") pour tous les salariés ou agents d'une entreprise ou d'une collectivité, afin de les acculturer à la menace et aux bonnes pratiques numériques

Constat : *les salariés ou agents ne connaissent pas suffisamment les modalités concrètes des cyberattaques, les moyens de les éviter à chaque niveau par des mesures élémentaires, ainsi que certaines conséquences de ces attaques.*

Il s'agirait donc d'**évoquer dans chaque structure les conséquences envisageables d'une cyberattaque, grâce à une simulation conduite une fois par an (sur le modèle de l'alerte incendie)** en modifiant les thématiques d'alerte chaque année et se formant de manière adéquate pour l'éviter.

Cette "alerte incendie cyber", organisée simplement par tout employeur sur la base d'un kit pédagogique en ligne (par Cybermalveillance.gouv.fr, par exemple), permettrait de mieux faire comprendre de façon simple les ressorts à l'œuvre lors de l'occurrence d'une attaque informatique. Pour les structures plus matures, cette séquence aurait vocation à devenir un véritable exercice de cyberattaque, à même de tester, soit le "mode dégradé" de l'organisation, soit les plans de continuité et de reprise de l'activité (PCA/PRA) pour les structures les plus matures. Des productions audiovisuelles ou infographiques de qualité (modèle de la *Hack Academy*), réalisées par des professionnels et financées par la puissance publique, permettraient de véhiculer un message simple, homogène et efficace. La mise en place d'une héroïque dédiée (des personnages bien identifiés mettant en valeur les bonnes pratiques) appuierait probablement la mémorisation des messages. En outre, le prestataire qui procéderait au diagnostic[174] de l'entité (en amont de sa déclaration de maturité) pourrait lui fournir des conseils et des recommandations pour organiser au mieux cette journée "d'alerte incendie cyber".

Si, pour les entités matures, cette simulation serait l'occasion de tester leur organisation de crise, cette dernière inciterait les entités moins matures à se remettre en question et à commencer à réfléchir à un plan de préparation pour continuer à fonctionner en cas de cyberattaque. Les bilans tirés par les petites entreprises et collectivités locales de ces "alertes incendie cyber" annuelles gagneraient aussi à faire l'objet d'un partage d'expérience.

Pour éviter de mettre en place une nouvelle obligation de l'employeur, le système de badges vise, à partir du niveau "graphite", à inclure un critère relatif à l'organisation annuelle de cette "alerte incendie-cyber", ou à des exercices plus perfectionnés. Néanmoins, ce dispositif pourrait devenir obligatoire à terme (par exemple, quelques années après la mise en place du système de badges), afin de poursuivre sur la durée l'acculturation du plus grand nombre aux menaces numériques, omniprésentes et évolutives.

[174] *Diagnostics in situ et audits.*

Recommandation 6 :

Instaurer une fonction de conseiller à la sécurité numérique (CSN) auprès de chaque responsable de structure (dirigeant d'entreprise ou élu) pour accompagner celui-ci sur les questions de cybersécurité

Constat : *le RSSI a pour mission de conseiller, dans cette matière à l'apparence fortement technique qui peut repousser les néophytes. Mais ces fonctions, qui connaissent une forte tension sur le marché de l'emploi, bénéficient d'une valorisation salariale importante que toute structure ne peut s'offrir (surtout à l'écart des grandes villes). Même mutualisé entre plusieurs sites ou structures, son coût reste élevé, et quelqu'un éloigné du fonctionnement habituel de la structure aura peut-être une moindre écoute du dirigeant.*

Le responsable[175] de la sécurité des systèmes d'information

D'après l'ANSSI[176] , un RSSI :

- assure le pilotage de la démarche de cybersécurité sur un périmètre organisationnel et/ou géographique au sein de l'organisation;
- définit ou décline la politique de sécurité des systèmes d'information;
- s'assure de la mise en place des solutions et des processus opérationnels ;
- définit ou décline la politique de sécurité des systèmes d'information ;
- assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte de la direction.

Il est généralement titulaire d'un diplôme de niveau BAC+4 à BAC+5 en informatique, et a un statut de cadre ou cadre supérieur.

En l'absence d'un RSSI interne ou externe, un conseiller à la sécurité numérique (CSN) pourrait être chargé d'accompagner le dirigeant de TPE/PME ou de petite collectivité dans la gestion des risques numériques et de la cybersécurité, en s'appuyant sur une culture de la sécurité numérique, sans nécessairement être un expert du domaine.

Ce poste de conseiller n'est pas un poste supplémentaire, mais la désignation (ou plutôt le volontariat) d'une personne choisie en interne, dans la gouvernance (au sein de l'équipe de direction, ou une personne ayant déjà un rôle de conseil auprès du dirigeant).La nomination d'un CSN serait requise pour toutes les entités à partir du niveau "bronze" du système de labellisation présenté *supra.* Ce CSN jouerait également le rôle de référent[177] cybersécurité pour l'ensemble de l'entreprise ou de la collectivité, sous la supervision éventuelle d'un RSSI mutualisé entre plusieurs entités.

Sans profil technique adéquat en interne, une compétence juridique (directeur juridique, juriste d'entreprise) pourrait être la plus appropriée pour remplir ce rôle, en raison des risques juridiques associés à la matière en cas

[175] *Le terme de "responsable" peut laisser à supposer au dirigeant qu'il transfère sa responsabilité juridique à ce spécialiste; tel n'est pas le cas.*

[176] *https://www.ssi.gouv.fr/uploads/2021/10/anssi-profils_de_la_cybersecurite-marche_ouvert-rssi.pdf*

[177] *https://www.assemblee-nationale.fr/dyn/15/rapports/cion_def/l15b1141_rapport-information#*

d'insuffisance. Pour former ces conseillers à la sécurité numérique, il conviendrait de s'appuyer sur la formation de "Référent cybersécurité TPE-PME" se déroulant sur 5 jours, au titre du budget de formation des entreprises, administré vers les opérateurs de compétences (OPCO). Parallèlement, l'un des dirigeants devrait suivre un court module de sensibilisation (qui sera proposé par Cybermalveillance.gouv.fr), pour disposer d'un vernis suffisant pour comprendre les risques et la matière. Le fait d'avoir suivi le MOOC d'initiation à la sécurité numérique proposé par l'ANSSI (SecNumacadémie)[178] , est exigible à partir du niveau "bronze" dans le système de badges.

[178] https://secnumacademie.gouv.fr/

Axe 2

Coordonner les ressources, les outils et les prérogatives de chaque acteur aux échelles appropriées : nouveaux moyens nationaux et mutualisations locales

Recommandation 7 :

Mutualiser les compétences et les outils chez les acteurs de confiance publics et privés en charge de la cybersécurité afin de permettre une couverture complète du maillage territorial

Constat : *comme mentionné précédemment, force est de constater qu'il existe une grande hétérogénéité des acteurs et des initiatives engagées dans cette lutte, tout en regrettant la faible accessibilité aux expertises nécessaires, soit insuffisantes en nombre, soit trop chères pour les personnes morales concernées.*

La profusion[179] d'acteurs pouvant être mobilisés en faveur de la cybersécurité dit l'importance du sujet mais appelle également une coordination plus étroite des objectifs, des organisations et des moyens.

Dans cette optique et sans présumer des prérogatives spécifiques à chaque acteur, trois grandes catégories d'action sont ici proposées :

> ***La première consiste à proposer via un tiers de confiance la mutualisation d'offres de RSSI pour les rendre plus accessibles à toutes les structures en demande, quels que soient la taille de la structure ou son secteur d'activité.***

Certains territoires[180] sont en effet peu fournis en RSSI, véritables spécialistes de la cybersécurité, dont le recours même ponctuel peut représenter une véritable plus-value mais aussi un budget important.

Cette approche repose sur le modèle du RSSI en temps partagé, où un expert en sécurité informatique travaille pour plusieurs entités différentes, pouvant intervenir de un jour par semaine (ou moins) à plusieurs jours par semaine au sein de chaque structure.

[179] *Au niveau central (lien avec les acteurs non critiques) : tous les services régaliens et leurs bras opérationnels, dont les services de la Première Ministre (SGDSN, ANSSI, lien avec Cybermalveillance.gouv.fr), du Ministère de l'Intérieur (DGPN, DGGN, DGSI notamment), du Ministère de la Justice (juridictions spécialisées), du Ministère des Armées (DRSD notamment), du Ministère de l'Economie (DGT, DGE, TRACFIN, DNRED), du Ministère du Numérique (CampusCyber).*

Au niveau régional : la préfecture, la gendarmerie, les services de renseignement (SI, RT, DRSR), la délégation régionale de l'ANSSI, les douanes, le conseil régional (dont CSIRT); éventuellement le Campus Cyber, un OPSN, les chambres consulaires (commerce & industrie, artisanat, agriculture), les fédérations professionnelles. Au niveau départemental : la préfecture, la justice, la gendarmerie, la police, les services de renseignement (SI, RT), les douanes, les chambres consulaires; éventuellement le conseil départemental, un OPSN, les fédérations professionnelles.

Au niveau de l'intercommunalité : la sous-préfecture, la gendarmerie, la police, l'établissement public de coopération intercommunale, éventuellement un OPSN.

[180] https://www.institutmontaigne.org/publications/mobiliser-et-former-les-talents-du-numerique

Pour faciliter cette mutualisation, **les RSSI pourront être regroupés au sein de tiers de confiance organisés en réseau territorial.** Parmi ces tiers de confiance, on peut citer :

- les Opérateurs Publics de Services Numériques (OPSN), pour les collectivités;
- une structure dédiée, quelle que soit sa forme[181], pour les entreprises et les collectivités sans OPSN. Celle-ci pourrait être adossée aux CSIRT régionaux et pourrait bénéficier de subventions publiques[182] en soutien à la démarche.
- Cette mutualisation pourrait également s'étendre à un niveau départemental, par le biais des chambres consulaires par exemple, ou encore celui des fédérations professionnelles départementales.

Imposer un RSSI partagé peut s'avérer difficile, en particulier pour les collectivités locales compte tenu de leur principe de libre administration. Dès lors, il conviendra de l'encourager par le biais du système de badges qui en fait un critère obligatoire à partir du niveau "argent" (vivement recommandé pour toutes les ETI).

Afin de favoriser l'échange d'informations et le partage des bonnes pratiques, il est également proposé d'instaurer un comité annuel des RSSI à l'échelle régionale (piloté par l'acteur le plus engagé de la région, que soit le CSIRT, le campus cyber régional ou la préfecture de région). Ce comité permettrait de dresser un bilan des actions menées, d'échanger au sujet de l'état de la menace, de partager les bonnes pratiques et de renforcer la collaboration entre les différents acteurs concernés.

Enfin, le recours à un RSSI par les personnes morales, rendu possible par la mutualisation, pourrait faciliter la distribution de subventions publiques à

[181] Association, société d'économie mixte, groupement d'intérêt public...

[182] Soit par la collectivité support (le conseil régional, par exemple), soit indirectement par des subventions accordées par l'État pour le fonctionnement de la structure ou ses compétences mises en œuvre.

des fins d'accompagnement et d'ingénierie (tels que d'ores et déjà pratiqués par des établissements dépendant de l'État ou par certains conseils régionaux pour la phase de diagnostic).

> ***La deuxième catégorie d'action concerne le regroupement des achats de solutions numériques et de matériels informatiques pour en diminuer les coûts et identifier des produits sélectionnés dont le déploiement est accompagné (notion de pack)***

Le regroupement des achats en matière de produits de cybersécurité vise à réduire les coûts et à faciliter l'adoption de produits sélectionnés pour leur efficacité, notamment en proposant des packs[183] assortis d'un accompagnement pour leur déploiement. Plusieurs mesures peuvent être mises en place pour atteindre cet objectif.

Le modèle des licences mutualisées[184] de l'ANSSI a fait ses preuves et pourrait justifier de sanctuariser un financement annuel modeste de 5M€, pour servir les communes avec OPSN[185]. Ce dispositif devrait également être assorti d'objectifs en matière de niveau de badge pour la déclaration de maturité. Par exemple, dans les prochaines années, toutes les collectivités de taille moyenne devraient avoir atteint le niveau "argent", tandis que toutes les petites collectivités devraient avoir atteint le niveau "bronze".

[183] Il s'agit de soutenir l'acquisition, par les structures encharge de la transformation numérique des collectivités,de produits et services mutualisés pour leurs adhérents. Le dispositif est accessible aux structures de mutualisation en charge de l'accompagnement à la transformation numérique des collectivités territoriales. Il s'agit par exemple des opérateurs publics de services numériques, des centres de gestion départementaux, des syndicats mixtes en charge du numérique. Seules les structures publiques, associatives ou les groupements d'intérêt public pourront être subventionnés, comme le précise l'ANSSI.

[184] Le dispositif de licences mutualisées porté par l'ANSSI a démontré toute son efficacité : 5,2M€ ont suffi pour couvrir 11 000 communes avec seulement 27 dossiers administratifs, en opérant un déploiement mutualisé via les OPSN.

[185] Il s'agit par exemple de systèmes de sauvegardes, coffre-fort numériques ou services managés (solutions intégrées de sécurité: patches automatiques dont antivirus nouvelle génération [EDR], protection des réseaux [firewall], détection de vulnérabilités et sécurisation des annuaires, sensibilisation au phishing [campagnes de faux mails], analyse de courriels douteux).

Pour faciliter le regroupement des achats, les OPSN pourraient être mobilisés pour les collectivités locales membres, tandis que les structures adossées aux CSIRT régionaux pourraient intervenir pour les entreprises (et les collectivités locales sans OPSN). Cela paraît d'autant plus pertinent que l'ANSSI dote chaque CSIRT régional d'une subvention annuelle de 1M€, pour chacune des trois premières années de fonctionnement, système qui gagnerait à être pérennisé pour les 5 prochaines années et sur l'ensemble du territoire (pour un budget d'environ 15M€ par an) afin de viser la complétude maximale.

Les centrales d'achat et d'identification des expertises peuvent jouer un rôle clé dans cette démarche, en fournissant notamment des produits informatiques et de cybersécurité à certaines collectivités (comme dans le secteur hospitalier). Il convient alors que les centrales d'achat, au-delà des critères de valeur technique et de prix des produits qu'ils proposent, veillent à prendre en compte les critères de solutions de confiance, de réversibilité et de simplicité de déploiement des produits proposés. Ces critères devraient faire l'objet d'une attention particulière par tout opérateur réalisant ses achats sur fonds publics.

Enfin, il est essentiel de mutualiser les ressources d'ingénierie, d'accompagnement au déploiement et de maintien en condition (telles que le déploiement automatique des mises à jour de sécurité) via les mêmes canaux que ceux utilisés pour le regroupement des achats. Cette approche permettra d'optimiser les coûts et de garantir un niveau de sécurité adéquat pour l'ensemble des structures concernées.

> ***La troisième catégorie d'action concerne l'identification d'un interlocuteur privilégié au niveau territorial capable de fédérer les différentes actions requises en matière de cybersécurité. Les CSIRT régionaux apparaissent aujourd'hui naturellement comme ces interlocuteurs possibles.***

Issus d'un projet du plan France Relance en 2021, les CSIRT régionaux sont des centres de réponse aux incidents cyber au profit des entités implantées sur le territoire régional. Ils traitent les demandes d'assistance des acteurs de

taille intermédiaire (ex : PME, ETI, collectivités territoriales et associations) et les mettent en relation avec des partenaires de proximité : prestataires de réponse à incident et partenaires étatiques.

L'émergence de ces CSIRT doit permettre de fournir localement un service de réponse à incident de premier niveau gratuit, complémentaire de celui proposé par les prestataires, la plateforme Cybermalveillance.gouv.fr et des services des CERT sectoriels.

Les équipes CSIRT portent également des missions de prévention, sensibilisation et d'accompagnement dans la montée en maturité des acteurs de leurs territoires. Les CSIRT régionaux ont pu bénéficier d'un financement ainsi que d'un accompagnement méthodologique sous la forme d'un parcours d'incubation. Le dispositif est constitué de 12 CSIRT régionaux, parmi lesquels 7 sont d'ores et déjà opérationnels[186].

Les CSIRT régionaux sont portés par les conseils régionaux, dans des formes juridiques diverses. Sur le terrain, les structures ont une variabilité importante. Les CSIRT peuvent coordonner leurs efforts avec des Agences régionales dédiées ou des Campus Cyber régionaux lorsqu'ils existent ou encore des associations. Les Campus Cyber régionaux (dont le nom peut différer) sont chargés de l'animation de l'écosystème de cybersécurité, du développement de la filière et de l'appui à la recherche et à l'innovation.

En Bourgogne-Franche-Comté, le CSIRT, en charge de la réponse à incidents et de l'assistance aux personnes morales, collabore étroitement avec l'ARNIA, l'Agence Régionale du Numérique et de l'Intelligence Artificielle. Ce type d'organisation peut constituer un modèle intéressant.

C'est donc bien à l'échelle régionale qu'il paraît opportun de s'organiser pour porter des offres de compétences mutualisées (telles des RSSI en temps partagé ou de l'ingénierie), **dans une logique d'accompagnement**

[186] *Normandie, Bourgogne- Franche-Comté, Centre-Val de Loire, Grand-Est, Hauts de France, Nouvelle Aquitaine et Occitanie.*

plébiscitée par les acteurs les moins préparés. La réalité du terrain invite à proposer que les CSIRT soient les interlocuteurs privilégiés de ces efforts, quels que soient les acteurs participant à cette lutte conjointe.

Le CSIRT régional de Bourgogne-Franche-Comté

Ouvert le 3 octobre 2022 avec un effectif de 4 personnes, après un programme d'incubation au sein de l'ANSSI, le CSIRT de Bourgogne-Franche-Comté a été le second à être opérationnel (après celui de Normandie). Comme tout CSIRT régional, il conserve un lien fonctionnel fort avec l'ANSSI, dans le suivi de son activité (échelon central) comme dans l'animation régionale de la filière (délégation régionale). A ce titre, l'outil pourrait avoir une légitimité renforcée dans les informations qu'il diffuse à d'autres CERT.

En l'absence d'un répertoire national des entreprises de cybersécurité, un recensement régional a pu être effectué[187], pour dénombrer 400 acteurs travaillant dans la région (dont 8 sont purement locaux). 7 sont labellisés ExpertCyber par Cybermalveillance.gouv.fr; il s'agit typiquement de PME d'informatique qui ont ajouté une compétence en matière de cybersécurité. La région ne compte aucun prestataire local d'un niveau supérieur.

En moyenne, le CSIRT réalise une quinzaine d'accompagnements de collectivités et entreprises par mois, ce qui est encore peu mais ce volume augmente en permanence, du fait d'une meilleure connaissance de l'outil et du partage d'informations

[187] Par tri des numéros de SIRET, puis des numéros d'APE, puis recherches complémentaires.

(de gendarmes, par exemple) vers le CSIRT, s'agissant de signalements de cyberattaques. L'accompagnement[188] se fait en heures ouvrées, ce qui correspond pour l'instant aux périodes de découverte des attaques[189]. Un devoir de confidentialité est imposé à ses personnels, et ses systèmes sont dissociés du reste du conseil régional. L'outil semble donc adapté à sa mission.

[188] Le CSIRT ne se déplace pas pour ne pas prendre la place des prestataires, ne communique pas et ne réalise pas les déclarations légales qui incombent au responsable de la structure, mais accompagne ces démarches.

[189] Schématiquement, les cyberattaques auraient plus souvent lieu entre le vendredi après-midi et le dimanche, et ne seraient découvertes dans les petites structures que le lundi.

L'agence régionale du numérique et de l'intelligence artificielle (ARNIA)

L'ARNIA est un groupement d'intérêt public (GIP, sous la tutelle du conseil régional), créé en 2008 après l'instauration d'une première plate-forme régionale dématérialisée des marchés publics. Elle compte aujourd'hui 1900 adhérents, pour fournir des outils informatiques à moindre coût (site web, tiers de transmission...), et surtout aider à la transition numérique.

Depuis le printemps 2023, l'agence porte à titre d'OPSN[190] des offres mutualisées à valeur ajoutée, sur la base d'appels d'offres commerciales. Les clients sont principalement des collectivités,

[190] Il s'agit de l'OPSN de référence pour les 8 départements de la région. Les chambres consulaires, quant à elles, seraient plutôt concentrées sur les questions de diagnostic ou d'audit.

pour des solutions qui concernent la sauvegarde (datacenter local, sauvegarde quotidienne avec 14j de sauvegarde, interface de restauration), le coffre-fort numérique, la sécurisation des postes de travail, les services managés[191] et téléphonie mobile. Outre le coût maîtrisé permis par la mutualisation, l'agence utilise certains critères de qualité et de souveraineté pour sélectionner les offres. Par exemple, les données doivent être hébergées en France, le firewall est qualifié par l'ANSSI, comme le coffre-fort de mot de passe (qui fait partie des licences mutualisées de l'ANSSI).

[191] *Patches automatiques dont antivirus nouvelle génération (EDR), protection des réseaux (firewall), détection de vulnérabilités et sécurisation des annuaires (avec l'ANSSI), sensibilisation au phishing (campagnes de faux mails), analyse de courriels douteux, sensibilisation et formation.*

Recommandation 8 :

Faciliter le signalement des attaques cyber via une "Plateforme de Signalement des faits Cyber", base de données commune aux différents services publics compétents en matière de cybersécurité, permettant un suivi consolidé

Constat : *les nombreux acteurs publics et privés partagent généralement de manière informelle certaines informations sur les menaces et les attaques dont ils font les frais. Ils le font sur la base de canaux différents, selon ce à quoi ils ont accès ou connaissance.*

Il existe ainsi 4 sites internet de signalement pour le hameçonnage (*phishing*), 3 plateformes de signalement de délinquance numérique propres à la police et à la gendarmerie (dont une de plainte en ligne), 1 plateforme de pré-plainte en ligne propre au ministère de l'Intérieur, sans oublier les systèmes de signalement propres à chaque institution spécialisée disposant d'une compétence cyber.

Cependant, les victimes déposent peu plainte[192] et, lorsqu'elles décident de le faire, ne trouvent pas toujours l'accueil escompté lorsqu'elles se déplacent pour des formalités pouvant être longues. En outre, le résultat judiciaire est incertain et peut être long à venir : on note de nombreux classements sans suite faute d'informations suffisantes et une coopération internationale est souvent nécessaire.

Une conséquence de la coexistence de nombreux services publics en charge de la cybersécurité est l'absence d'une vision d'ensemble sur la réalité de la menace cyber, par catégorie de victimes ou de secteurs. Parce que le périmètre de ces services publics ne couvre pas tout le spectre existant, des entreprises qui sont victimes n'ont pas forcément l'obligation d'en référer à l'ANSSI (si elles ne sont pas dans son périmètre), tandis qu'elles ne vont pas forcément (voire très probablement pas) venir chercher de l'assistance sur Cybermalveillance.gouv.fr .

Tous ces éléments freinent la capacité commune d'analyse et de réponse.

> ***Instaurer une unique "plateforme de signalement des faits cyber", afin de constituer une base de données commune aux différents services publics ayant une compétence cyber***

[192] *Le nouvel article L.12-10-1 du Code des assurances (issu de la LOPMI) va davantage conduire les entreprises assurées à déposer plainte, pour garantir la validité des clauses du contrat. Néanmoins, très peu d'entreprises sont assurées.*

La mise en place d'une "plateforme de signalement des faits cyber" sous la forme d'une base de données communes aux différents services publics "cyber" induirait, d'une part, une rationalisation/simplification des processus de signalements en cas d'incidents de sécurité numérique pour les entreprises et les collectivités et, d'autre part, permettrait à la puissance publique de développer une meilleure connaissance de la menace cyber (cf. annexe 2).

Dans l'esprit de la démarche du "17 cyber", initiée par le ministère de l'Intérieur en 2023[193], la mise en place d'une telle plateforme nécessiterait la création d'un site Internet unique. Cette interface pourrait saisir les services appropriés (sans action supplémentaire de la part du signalant); elle pourrait aussi se substituer aux multiples moyens de signalement existants. Il serait important de valoriser l'expertise de Cybermalveillance.gouv.fr pour en faire un véritable guichet unique des victimes. Ce site est en effet de plus en plus connu et permettrait d'unifier les différentes plateformes déjà existantes, pré-plaintes et plaintes en ligne pour les incidents cyber, en proposant un canal simple et unique de saisie et de remontée des informations liées aux victimes, y compris pour les personnes morales.

Une telle centralisation suppose au minimum, de façon dédiée : des moyens humains (quelques dizaines de personnes pour l'administration, l'analyse, la communication), immobiliers et matériels (notamment un système d'information robuste, à créer). Le coût de fonctionnement en serait probablement d'environ 5M€ par an.

Cette situation pourrait être transitoire, constituant un simple filtre d'orientation, pour ne présenter qu'une seule interface de saisine aux signalants. À terme, cette structure pourrait héberger les capacités d'analyse (notamment technique et judiciaire) et de réponse des différents services ayant déjà

[193] Dans son discours du 10 janvier 2022 à Nice (06), le Président de la République a exprimé l'objectif d'un interlocuteur unique pour les victimes de cyberattaques. Cet objectif a été pris en compte par la loi 2023-22 du 24 janvier 2023 d'orientation et de programmation pour le ministère de l'intérieur. Les contours précis du projet ne sont pas encore connus, mais il s'agira au minimum d'un concept de guichet unique. La plainte en ligne existe par ailleurs (plateforme THESEE, pour les personnes physiques uniquement, victimes de certains faits en ligne), pour certains faits précis, et la visioplainte est expérimentée.

une compétence dans le domaine. Il ne s'agit alors pas de moyens supplémentaires, mais d'un transfert vers une entité, nécessairement régalienne, de coopération inter-services[194]. Dans ce modèle intégré, c'est le chantier juridique qui peut se révéler le plus lourd, si un fichier unique (semblable à un fichier de police) devait se substituer aux multiples fichiers, registres et traitement de données existants. Un tel service pourrait avoir sa place sous l'égide des services de la Première Ministre, en raison de la surface et de la sensibilité des compétences ainsi rassemblées.

Comme il existe à ce stade peu de leviers incitatifs, la déclaration d'une cyberattaque ou d'un incident sur la plateforme serait facultative. La précision, la sincérité et la fréquence des déclarations pourraient également constituer un faisceau d'indices sur le niveau de rigueur, de transparence et de bonne foi d'une structure, en cas de contrôle administratif ou d'enquête judiciaire. Néanmoins, cette déclaration sera potentiellement obligatoire pour les quelque 10 000 entités qui entreront dans le champ d'application de la directive NIS 2. Un tel système, dont le recueil, le traitement, l'analyse, l'exploitation et le partage des informations serait en partie automatisée, faciliterait probablement le passage à l'échelle pour les services publics. Si cette phase amont était facilitée, la phase aval le serait également par conséquence.

Ainsi, le CSIRT compétent (lieu d'implantation de la collectivité ou entreprise) sera automatiquement informé[195] (par notification) lors de la déclaration d'une cyberattaque ou d'un incident sur la plateforme, afin d'accélérer l'aide à la remédiation. Les CSIRT doivent d'ailleurs pouvoir consulter la base de données unique, et l'alimenter.

Le formulaire de déclaration d'une cyberattaque pourrait également inclure, sur le modèle des plateformes "*No more ransom" d'Europol*[196]" ou "*ID Ran-*

[194] Le modèle des groupes d'intervention régionaux (GIR), par exemple, fait travailler dans le même service policiers, gendarmes, douaniers, administration fiscale, URSSAF...

[195] Au titre de l'étude de terrain du présent rapport, les gendarmes de Normandie comme le CSIRT de Bourgogne-Franche-Comté ont indiqué que les échanges existent déjà et sont fluides. Mais ils sont informels et ne sont pas toujours immédiats.

somware" ou "*MalwareHunterTeam*", un encart spécifique pour les attaques par rançongiciels. Ce formulaire permettrait aux victimes de téléverser quelques fichiers chiffrés, ainsi que le message de demande de rançon, afin de permettre d'identifier automatiquement la souche du rançongiciel utilisé et de diriger la victime, vers un logiciel de déchiffrement[197] (s'il existe). Les entités qui ne sont pas obligées de déclarer ou signaler un incident de sécurité auquel elles auraient fait face pourraient être encouragées par l'application de la politique du "droit à l'erreur", permettant de ne pas pénaliser (en matière de sanction administrative seulement) celles qui auraient été de bonne foi[198].

Ce même canal sera également utilisé pour recueillir les déclarations des personnes morales[199] concernant leurs déclarations de maturité cyber, visant à l'obtention des badges .

[196] https://www.nomoreransom.org/crypto-sheriff.php?lang=fr

[197] *Si ce dernier n'est pas disponible, il serait possible de laisser son adresse e-mail afin d'être prévenu automatiquement s'il l'est un jour. 193 Ainsi, la structure n'encourra pas de sanction administrative si la faille exploitée dans le cadre d'une cyberattaque n'aurait pas dû être présente - ceci n'empêchant pas le contrôle du reste de ses systèmes, et la vérification d'éventuelles fausses déclarations.*

[198] *Ainsi, la structure n'encourra pas de sanction administrative si la faille exploitée dans le cadre d'une cyberattaque n'aurait pas dû être présente - ceci n'empêchant pas le contrôle du reste de ses systèmes, et la vérification d'éventuelles fausses déclarations.*

[199] *Des vérifications des éventuelles fausses déclarations seront effectuées lors de contrôles inopinés ou réac tifs, c'est-à-dire menés à la suite de la déclaration d'un incident sur la plateforme par l'entité.*

L'engagement de responsabilité de la personne morale et du dirigeant

En cas de manquement, trois types de responsabilités (parfois cumulatives) existantes sont à distinguer et peuvent entraîner des sanctions de différentes natures :

- la sanction administrative : elle est décidée par une autorité de contrôle à l'égard d'une personne morale ;
- l'indemnisation pour engagement de responsabilité civile : elle est décidée par une juridiction civile et peut concerner une personne morale comme une personne physique ;
- la sanction pénale : elle est décidée par un juge pénal, et peut concerner une personne morale comme une personne physique (dirigeant, élu, responsable, comme tout usager ayant commis une imprudence ou négligence dans sa fonction ayant entraîné des conséquences pour autrui).

Les services régaliens disposant d'une compétence cyber auront accès au contenu de la plateforme selon la règle habituelle du droit et du besoin de connaître de ces informations, en fonction des finalités propres à chaque service.

D'un point de vue pénal, en s'inspirant du modèle américain de l'IC3 (cf. *supra*), il s'agirait ainsi de procéder à une analyse préalable, avant de catégoriser l'incident comme une simple "main courante", ou d'orienter la victime vers une plainte dans le service le plus adapté (permettant alors un rendez-vous avec un enquêteur spécialisé, la mise en oeuvre d'un accompagnement adapté et de meilleures garanties de confidentialité).

En complément de cette plateforme de signalement, un "Observatoire de la menace numérique" pourrait être mis en place. Cet observatoire, quel que soit son rattachement administratif ou politique, doit s'appliquer en priorité à rassembler, compiler, trier, catégoriser et analyser les menaces, pour dégager des réponses pouvant être coordonnées. Pour permettre une analyse à la fois centralisée et partagée entre les acteurs concernés, ainsi qu'une meilleure base statistique, il pourrait s'adosser à la plateforme de signalement. Cela permettrait de manier des quantités plus importantes d'informations anonymisées et "raffinées" (grâce à un traitement automatique sur la base d'algorithmes de tri, puis de manière manuelle pour plus de précision). Les acteurs

privés, notamment les assureurs, pourraient bénéficier de cette démarche et y prendre part (partage croisé d'informations) via la participation du Campus Cyber et de Cybermalveillance.gouv.fr, par exemple.

Le coût annuel d'un tel observatoire, sur la base d'une vingtaine d'agents à l'échelle nationale, pourrait avoisiner les 2M€ afin d'aider à la sécurisation du tissu économique et social.

La plateforme en tant qu'instrument régalien de centralisation et de coordination d'une part, l'observatoire en tant que lieu de centralisation des données qualitatives et quantitatives sur les attaques cyber et incluant des acteurs publics et privés, pourraient constituer les deux piliers d'une visibilité tant stratégique qu' opérationnelle.

Recommandation 9 :

Renforcer les moyens et l'organisation des acteurs de la lutte contre la cybercriminalité dans une logique de proximité, en mettant l'accent sur la prévention et sur la répression

Constat : *En termes de prévention, il est important de comprendre que toutes les structures concernées ne pourront se tourner vers le secteur privé, en forte tension. Le secteur privé lui-même se détourne majoritairement des petites structures. En effet, dans les territoires moins attractifs, parfois reculés, on constate une hétérogénéité de service qui va rarement jusqu'au dernier kilomètre. L'initiative publique doit compléter l'initiative privée là où elle ne va pas. Dans la phase d'investigation, la maturité fait également défaut. Ainsi, on constate que les victimes de cyberattaques ne prennent pas rendez-vous avec des enquêteurs spécialisés et n'ont pas toujours l'accompagnement adéquat. Les affaires à faible enjeu peuvent rapidement être classées ou arrivent dans des juridictions insuffisamment armées pour traiter ce type de contentieux très spécifique.*

> ***Développer une logique de cybersécurité de proximité et densifier les acteurs de terrain de la chaîne publique pour mieux prendre en compte les risques cyber et leurs particularismes (masse, technicité, criticité)***

S'agissant de la prévention, le Ministère de l'Intérieur dispose d'un maillage territorial et d'une puissance opérationnelle et de formation lui permettant de traiter une partie des missions associées à la menace numérique. A titre d'exemple, des référents chargés de la prévention technique de la malveillance accompagnent collectivités et entreprises dans le durcissement de leur sécurité physique, sous l'égide de la police ou de la gendarmerie. Un tel modèle pourrait utilement être dupliqué en cellules de prévention des risques cyber. Un format de 5 personnels par département (en moyenne), par exemple[200] constituerait une force de frappe dans un premier temps suffisante, pour un coût moyen annuel à l'ensemble du pays de 35M€.

L'intérêt de développer une forte démarche de prévention est majeur : une structure prévenue, avec des personnels acculturés, représente un bien moindre risque d'être victime d'une cyberattaque, et donc une bien moindre activité pour le reste de la chaîne (judiciaire et de remédiation, notamment) qui doit être structurée.

Il existe actuellement une vraie perspective de recrutement et de formation d'enquêteurs numériques au sein du Ministère de l'intérieur.

Un budget[201] de 2M€ au sein de Cybermalveillance.gouv.fr permet d'accompagner les victimes. Son succès croissant, signe de l'augmentation des attaques et de sa pertinence dans la gestion des sollicitations, mériterait très certainement d'être renforcé proportionnellement afin de lui permettre de continuer à pouvoir maintenir et développer son offre de service.

[200] *A raison de 2 jours par entreprise ou collectivité, en moyenne (préparation du diagnostic, réalisation, analyse, restitution, sensibilisation du personnel de la structure), chaque personnel peut en traiter environ 100/an, soit 500 structures/an/département. Le format doit rester réaliste face au triptyque : capacité de formation des référents, demande locale, coût pour l'État.*

S'agissant des investigations de cyberattaques : lorsqu'elles sont de nature délictuelle, c'est principalement la section J3 du parquet de Paris, spécialisée dans le sujet de cybercriminalité, qui est saisie en première intention (notamment à partir des faits issus des plateformes actuelles et au titre de sa compétence nationale[202]). Le parquet a charge ensuite de redistribuer aux juridictions des territoires abritant les victimes les dossiers les concernant. Lorsque les cyberattaques relèvent de la criminalité organisée, ce sont les juridictions d'instruction régionales spécialisées qui sont généralement saisies. Considérant le bénéfice majeur du démantèlement de groupes cybercriminels, pour éviter de nombreuses nouvelles victimes, l'action judiciaire contre la cybercriminalité est fondamentale.

Au vu de l'évolution des volumes de cyberattaques, consacrer davantage de moyens humains à la thématique numérique pour les juridictions concernées pourrait avoir du sens[203] et permettre entre autres l'anticipation de futurs procès de masse liés à la cybercriminalité. Un total de 250 postes[204] pourrait représenter un coût annuel d'environ 20M€.

De fait, les évolutions récentes des menaces, tant dans leur volumétrie que dans leur mode de déploiement, appellent un ajustement des besoins et des organisations judiciaires afin d'allier une approche régalienne axée sur l'identification des risques, des intérêts stratégiques et des réglementations adéquates, et une approche plus opérationnelle sur le terrain afin d'instaurer une cybersécurité de proximité à même d'accompagner avec plus d'agilité les acteurs territoriaux de la prévention à la répression

[201] https://www.senat.fr/rap/r21-219/r21-219.html

[202] https://www.senat.fr/notice-rapport/1963/i1963_1964_0283-notice.html

[203] *Le projet de loi d'orientation et de programmation pour la justice, en cours de discussion au Parlement, prend en compte cette perspective.*

[204] *Soit en moyenne 2 postes par juridiction pénale du premier et du second degré (siège et parquet), ainsi que dans les juridictions interrégionales spécialisées, les services centraux (détachement) et les écoles de formation.*

Renforcer les moyens des services chargés de la conception, de la supervision et de la régulation

Autorité française en matière de sécurité numérique, l'ANSSI doit tout à la fois maintenir son niveau d'exigence technique, qui fait référence au plus haut niveau s'agissant de la certification et de la labellisation. Elle le fait sur un périmètre aujourd'hui stable. Or, la réglementation européenne devrait au moins décupler l'assiette des structures supervisées. L'ANSSI devra donc se doter des capacités d'analyse et de réponse en adéquation avec ces attentes démultipliées[20].

Autre enjeu connexe, la sécurisation des données personnelles est souvent déterminante dans la protection des systèmes, et constitue parfois la principale finalité des mesures de sécurité numérique. Le contrôle, et éventuellement la sanction de manquements à la sécurité des données personnelles, est une compétence de la CNIL. Ainsi, la CNIL pourrait être amenée à réaliser davantage de contrôles auprès de la multitude de structures concernées par les obligations du RGPD. Consolider les moyens de cette commission pour augmenter le nombre de contrôles devrait permettre d'augmenter également la prévention des atteintes aux données personnelles, en investissant dans la sécurité numérique.

[207] https://www.assemblee-nationale.fr/dyn/15/rapports/souvnum/l15b4299-t1_rapport-information

L'incidence d'une sécurité numérique insuffisante sur la sécurité des données personnelles

La protection des données personnelles est une impérieuse obligation. Elle concerne toute entreprise ou collectivité; or, la sécurité des données se trouve vite compromise si la sécurité numérique de la structure n'est pas assurée. Des données peuvent ainsi être subtilisées et publiées :

- des données fiscales, sociales, patrimoniales, matrimoniales dans une mairie (même petite) ou une structure de l'aide sociale ou de l'enfance ;
- des contrats ou procédés de fabrication dans une petite entreprise industrielle ;
- des historiques de voyages et références de documents d'identité dans des agences de voyage ;
- des données bancaires, assurantielles et patrimoniales dans des agences immobilières; - des historiques de déplacement dans des sociétés de taxi ;

Recommandation 10 :

Pérenniser le financement de l'effort public en faveur d'une sécurité numérique collective par un abondement vertueux des budgets

Constat : *Comme toute ambition stratégique qui se respecte, la visibilité des moyens à y consacrer participe de sa réussite. Dans le domaine de la cybersécurité, l'évolution rapide des menaces et la nécessité constante de s'adapter en temps réel rendent cet impératif de visibilité budgétaire encore plus crucial.*

Financer cet effort public grâce à une impulsion de l'État ou à des amendes infligées dédiées

Il convient de se doter des moyens appropriés à un tel enjeu de sécurité et de définir la provenance des financements nécessaires. Un examen rapide permet d'identifier d'ores et déjà deux voies possibles.

La première voie est nécessairement étatique, la sécurité du territoire relevant des autorités régaliennes qui doivent donc arbitrer la dépense en fonction des priorités. Nous estimons que le budget de lutte contre la cybermenace représente quelque 100M€ supplémentaires par an pour une couverture des territoires et des plus petits, avec un objectif de renforcement des moyens humains au niveau national et le maillage public adéquat.

En outre, l'ANSSI disposera de la prérogative d'infliger des amendes proportionnelles au chiffre d'affaires des structures qu'elle supervise, en application de la transposition de la directive NIS 2. On peut imaginer qu'une partie de ces amendes vienne, à terme, abonder le budget de lutte en faveur de la sécurité numérique.

La seconde voie serait éventuellement décentralisée, trouvant dans des acteurs dédiés des ressources redistribuables à la cause : ainsi, par exemple, des amendes de la CNIL qui pourrait constituer un expédient budgétaire facile d'accès[206].

Un tel modèle de financement serait dérogatoire[207] du droit commun car toute amende est versée traditionnellement au budget de l'État. Néanmoins, le principe d'affectation est déjà utilisé. On le voit à l'œuvre au profit de la MILDECA (Mission interministérielle de lutte contre les drogues et les conduites addictives) où les saisies de stupéfiants servent à financer la lutte contre la toxicomanie. On le voit également auprès de l'AGRASC, l'Agence de gestion et de recouvrement des avoirs saisis et confisqués, qui fait fructifier

[206] *La totalité des amendes décidées par la CNIL est de 101M€, actuellement versées dans le budget général de l'État. https://www.cnil.fr/fr/sanctions-et-mesures-correctrices-la-cnil-presente-le-bilan-2022-de-son-action-repressive*

[207] *https://www.thedigitalnewdeal.org/cybersecurite-vigile-de-notre-autonomie-strategique-2/*

les avoirs criminels. Le programme de sécurité routière, jugé priorité nationale, avait instauré la même logique de réinjection des amendes au service de la cause portée[208]. Il peut y avoir un intérêt à s'inspirer de ces exemples.

Une telle logique se veut avant tout pragmatique et en aucun cas une incitation à atteindre des objectifs annuels d'amendes.

Conclusion

Cette étude à la fois globale et territoriale a montré l'urgence d'une action coordonnée aux différentes échelles du territoire. L'expérience de terrain invite à un pragmatisme volontaire qui mobilise chaque acteur de la sécurité numérique à son juste niveau. `

Au niveau national, l'ANSSI porte l'ambition de la sécurité numérique nationale et promeut les solutions et outils les plus pertinents pour les acteurs concernés. Les services de l'Intérieur portent les enjeux de prévention et d'investigation, couplés avec la Justice pour la partie sanctions.

Au niveau local, les conseils régionaux, les préfectures et autres services de l'État, les chambres consulaires et les collectivités ont tous un rôle à jouer de sensibilisation, de formation, d'anticipation des attaques et de collecte d'informations. Le secteur privé a essentiellement une responsabilité d'accompagnement, d'ingénierie technique et de remédiation en cas de problème.

Les conditions clés pour un passage à l'échelle effectif et réussi reposent essentiellement sur l'articulation des efforts de ces différents acteurs en temps réel et la mobilisation rapide des moyens identifiés.

[208] En 2021, 88,5 % des recettes de contrôle automatisé de vitesse ont financé l'effort de l'État pour la sécurité routière, au travers de l'Agence de financement des infrastructures de transports de France, des collectivités territoriales, de la Délégation à la sécurité routière, du fonds de modernisation pour l'investissement en santé. Le reliquat de 11,5 % a servi au désendettement de l'État. https://www.securite-routiere.gouv.fr/ radars/chiffres-radars/recettes-des-radars

Côté entreprises et petites collectivités, la priorité est à la compréhension des enjeux, l'acceptation des accompagnements disponibles et la mise en place des outils proposés (diagnostic et mise à niveau personnalisée).

La conviction des professionnels du secteur est qu'il suffit de peu pour améliorer la sécurité des structures locales, pour autant que celles-ci en comprennent l'utilité et en acceptent les modalités pratiques. Le numérique irriguant désormais tous nos usages, la sécurité doit devenir un réflexe naturel, comme le port de la ceinture de sécurité dans les voitures ou la fermeture de la porte d'entrée de sa maison : un comportement de bon sens que personne ne remet en cause.

Annexe 1

Rétrospective des principaux dispositifs français et européens liés aux questions de cybersécurité

Année	Dispositif
2004	Création de l'European Network and Information Security Agency (ENISA) avec le règlement (CE) n°460/2004[201]
2005	Décision-cadre du Conseil de l'Union européenne relative aux attaques visant les systèmes d'information
2009	Création de l'ANSSI
2013	Publication de la première stratégie de cybersécurité de l'UE[202] Règlement UE N° 526/2013 concernant l'ENISA[203] Promulgation de la Loi de programmation militaire 2014 - 2018 (intégrant les enjeux de sécurité numérique au concept d'OIV)
2014	Mise en oeuvre du référentiel général de sécurité[204] (RGS)
2015	Publication de la stratégie nationale pour la sécurité numérique[205]
2016	Adoption de la directive européenne NIS[206] (*Network and Information Security*)
2017	Création du GIP ACYMA (Cybermalveillance.gouv.fr), avec de nombreuses initiatives depuis
2018	Nomination d'un délégué ministériel aux industries de sécurité et à la lutte contre la cybermenace Mise en oeuvre du règlement UE n°2016/679 ou Règlement général sur la protection des données (RGPD)
2018	Promulgation de la Loi de programmation militaire 2019 - 2025
2019	Adoption du règlement UE n°2019/881 ("Cyber Security Act") relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications règlement relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications[207] Lancement d'appels à projets (à destination des PME/start-up) dans le cadre du Grand défi Cyber
2020	Publication de la nouvelle stratégie européenne de cybersécurité[208] Proposition de directive européenne sur la résilience des entités critiques

[209] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32004R0460&qid=1685708225896
[210] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52013JC0001
[211] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32013R0526&qid=1685708573289
[212] https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/
[213] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf

[214] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.FRA&toc=OJ%3AL%3A2016%3A194%3ATOC 207 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.FRA&toc=OJ:L:2019:151:TOC

[215] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.FRA&toc=OJ:L:2019:151:TOC

[216] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

[217] *Le comité rassemble des représentants des entreprises, des acteurs publics, de la recherche et de la formation dans le domaine de la cybersécurité. Son objectif principal est de favoriser la coopération entre les différents acteurs de la filière pour renforcer la compétitivité de l'industrie française de la cybersécurité sur le plan national et international.*

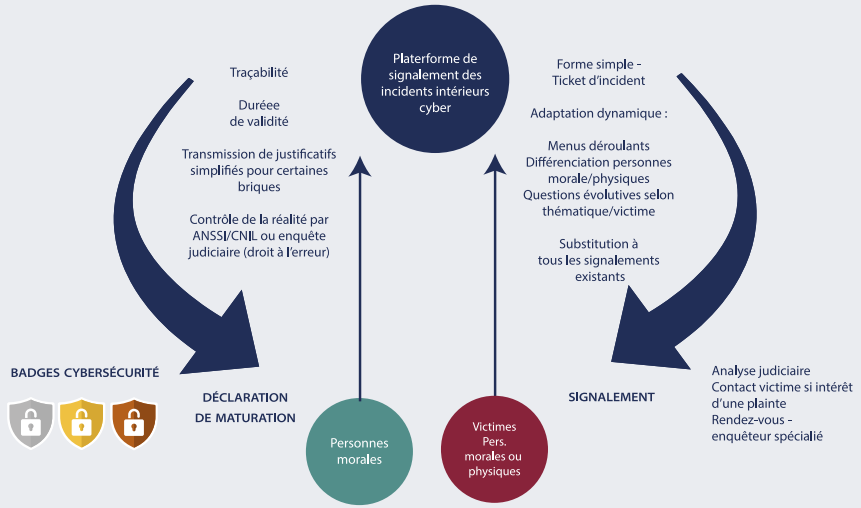
Année	Dispositif
2021	Décennie numérique de l'Europe (Digital compass 2030) Proposition de règlement européen sur l'intelligence artificielle Stratégie nationale d'accélération pour la cybersécurité Création du Campus Cyber Création du comité stratégique de filière cybersécurité[209] Création du Commandement de la gendarmerie dans le cyberespace (COMCYBERGEND) pour piloter l'action des unités antérieures
2022	Adoption de la directive européenne NIS/SRI 2 Adoption du règlement européen sur la résilience opérationnelle numérique (DORA) Paquet législatif sur les services numériques Adoption du règlement sur les marchés numériques (*Digital Markets Act* ou DMA) Proposition de règlement européen *Cyber Resilience Act* (CRA, cf. encadré supra) par la Commission européenne Proposition de règlement sur la gouvernance européenne des données Adoption de la Loi pour la mise en place d'un "cyberscore", une certification de cybersécurité des plateformes numériques destinée au grand public et mise en consultation par la DGE du projet d'arrêté d'application[210] [211]

[218] https://www.entreprises.gouv.fr/files/files/secteurs-d-activite/numerique/ressources/consultations/projet-arrete-cyberscore.pdf

[219] *Quand bien même le texte de loi présente le cyberscore sous la forme d'une certification de "cybersécurité", force est de constater que les critères retenus dans le projet d'arrêté d'application ont en réalité trait aux enjeux de souveraineté numérique (localisation datacenters hébergeant les données, d'exposition des données à des législations à portée extraterritoriale, etc.)*

Annexe 2

Principe de la plateforme de signalement des incidents intérieurs cyber



Annexe 3

Données sur le coût engendré par les rançongiciels

Le coût engendré par les rançongiciels est devenu un sujet de préoccupation majeure en raison de la capacité de ces logiciels malveillants à mettre un coup d'arrêt aux activités opérationnelles d'une entreprise.

En pratique, le coût économique des rançongiciels est difficile à quantifier avec précision car il dépend du nombre de victimes, du montant des rançons payées, mais aussi de la perte économique engendré par le blocage de l'accès aux ressources informationnels, qu'il soit temporaire ou permanent, l'impact sur les clients ainsi que sur la réputation de l'entreprise.

En dépit de ces difficultés, certaines études ont été menées pour tenter d'estimer l'impact financier de ces attaques, comme en témoigne les tableaux ci-dessous, tirés d'une étude d'Emsisoft réalisée en 2021 sur l'année 2020[212] et cités par le "Rapport économique 2023 du Président des États-Unis[213] ".

Les données qui ont permis de construire ces statistiques sont principalement issues des soumissions sur la plateforme d'identification de rançongiciel "ID Ransomware".

Le premier tableau présente la somme des demandes de rançons dans chaque pays, le deuxième tableau présente cette somme en excluant les particuliers, tandis que le troisième et dernier tableau ajoute aux rançons demandées les coûts associés à la remédiation. La colonne "Minimum Costs" correspond aux données issues directement des soumissions sur la plateforme "ID Ransomware", tandis que la colonne "Estimated Costs" correspond à ce nombre

[212] https://www.emsisoft.com/en/blog/38426/the-cost-of-ransomware-in-2021-a-country-by-country-analysis/
[213] https://www.whitehouse.gov/wp-content/uploads/2023/03/ERP-2023.pdf

multiplié par 4 (*Emsisoft faisant l'hypothèse qu'environ 25% des organisations public ou privé affectées par des rançongiciels recourent à la plateforme ID Ransomware*). La colonne "Inferred Costs per submission" correspond au montant moyen par soumission.

Selon Emsisoft, le coût des rançongiciels sur l'économie mondiale est en croissance sur les dernières années. En 2020, les États-Unis auraient été touchés à hauteur de 3682 Mds$, l'Italie 1387 Mds$, l'Espagne 1193 Mds$, la France 1135 Mds$, l'Allemagne 1011Mds$, le Royaume-Uni 677 M$, le Canada 659 M$, l'Australie 424 M$, l'Autriche 186 M$, la Nouvelle-Zélande 56 M$. L'exemple de ces quelques pays seulement suffit à illustrer l'ampleur à l'échelle mondiale.

Au niveau mondial, selon Emsisoft, 18 Mds$ au minimum auraient été demandés en rançon en 2020, tandis que le coût des interruptions d'activité afférents dans les secteurs privé et public s'est élevé à des milliards de dollars supplémentaires. Selon Emsisoft, environ 27 % des organisations et particuliers touchés auraient payé la demande de rançon, impliquant un gain minimal pour l'écosystème criminel de minimum 5 Mds$ en 2020.

Tableau 1 : Country-by-country breakdown – Home users included

Country	Total Submissions	Minimum Cost (USD)	Estimated Costs (USD)	Inferred Costs per submission (USD)
United States	23 661	$920 353 010	$3 682 228 067	$38 897
Italy	9 226	$346 729 130	$1 387 389 097	$37 582
Spain	8 475	$298 254 459	$1 193 709 500	$35 192
France	7 824	$283 816 080	$1 135 795 109	$36 275
Germany	7 138	$252 609 210	$1 011 001 498	$35 389

Country	Total Submissions	Minimum Cost (USD)	Estimated Costs (USD)	Inferred Costs per submission (USD)
U.K.	4 788	$169 182 845	$677 113 461	$35 335
Canada	4 257	$164 772 274	$659 246 267	$38 706
Australia	2 775	$105 978 531	$424 034 780	$38 190
Austria	1 254	$46 643 868	$186 645 857	$37 196
New Zealand	399	$14 230 333	$56 951 495	$35 665
Total (All countries)	506 185	$18 658 009 233	$74 632 036 933	$36 860

Tableau 2 : Private and public sector-only – Home users excluded (ransom costs only)

Country	Total Submissions	Minimum Cost (USD)	Estimated Costs (USD)	Inferred Costs per submission (USD)
United States	15 672	$596 436 809	$2 385 747 238	$38 057
France	4 476	$159 738 887	$638 955 546	$35 688
Spain	4 088	$151 309 229	$605 236 914	$37 013
Italy	3 835	$147 376 932	$589 507 727	$38 429
Germany	3 747	$132 558 050	$530 232 201	$35 377
Canada	3 236	$123 697 351	$494 789 403	$38 225
U.K.	2 718	$93 475 142	$373 900 568	$34 391
Australia	2 072	$79 951 174	$319 804 695	$38 586
Austria	819	$32 252 920	$129 011 681	$39 381
New Zealand	265	$9 906 552	$39 626 209	$37 383

Tableau 3 : Private and public sector-only – Home users excluded (ransom + downtime costs)

Country	Total Submissions	Minimum Cost (USD)	Estimated Costs (USD)	Inferred Costs per submission (USD)
United States	15 672	$4 893 699 209	$19 574 796 838	$312 257
France	4 476	$1 387 058 087	$5 548 232 346	$309 888
Spain	4 088	$1 272 238 829	$5 088 955 314	$311 213
Italy	3 835	$1 198 933 932	$4 795 735 727	$312 629
Germany	3 747	$1 159 985 450	$4 639 941 801	$309 577
Canada	3 236	$1 011 008 551	$4 044 034 203	$312 425
U.K.	2 718	$838 750 742	$3 355 002 968	$308 591
Australia	2 072	$648 093 574	$2 592 374 295	$312 786
AustrIA	819	$256 822 720	$1 027 290 881	$313 581
New Zealand	265	$82 569 552	$330 278 209	$311 583

Annexe 4

Règles de sécurité applicables par les OSE en application des textes de transposition de la directive NIS

Le tableau ci-dessous présente les 23 règles de sécurité mentionnées à l'annexe I de l'arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du 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 (https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037444012). Ces différents textes ont été adoptés afin de transposer la directive NIS.

	Catégorie	Nom de la règle	Résumé de la règle
1	Gouvernance	Analyse de risque	L'opérateur de services essentiels (OSE) doit effectuer une analyse de risque de ses systèmes d'information essentiels (SIE) dans le cadre de l'homologation de sécurité prévue par la règle 3
2	Gouvernance	Politique de sécurité	L'OSE doit élaborer, mettre en œuvre et mettre à jour une politique de sécurité des réseaux et systèmes d'information (PSSI) qui décrit les procédures et les moyens organisationnels et techniques mis en œuvre pour assurer la sécurité des systèmes d'information essentiels, en définissant les objectifs, les orientations stratégiques, les plans de sensibilisation et de formation, les mesures de sécurité, les procédures de détection et de traitement des incidents, les procédures de gestion de crise, ainsi que la procédure d'homologation de sécurité, et doit approuver cette PSSI formellement et produire un rapport annuel sur sa mise en œuvre et l'état des risques pour l'ANSSI
3	Gouvernance	Homologation de sécurité	L'OSE homologue la sécurité de chaque système d'information essentiel en suivant une procédure d'homologation détaillée, qui comprend notamment une analyse de risques, des mesures de sécurité et des audits de sécurité, et réexamine la validité de l'homologation au moins tous les trois ans.
4	Gouvernance	Indicateurs	L'OSE évalue et tient à jour des indicateurs relatifs à la sécurité des systèmes d'information essentiels, incluant notamment des indicateurs relatifs aux droits d'accès des utilisateurs et à l'administration des ressources, et communique ces informations à l'Agence nationale de la sécurité des systèmes d'information sur demande.
5	Gouvernance	Audits de la sécurité	L'OSE doit réaliser un audit de sécurité pour chaque système d'information essentiel dans le cadre de l'homologation de sécurité, en se basant sur un référentiel d'audit, afin de vérifier l'application et l'efficacité des mesures de sécurité, évaluer le niveau de sécurité et formuler des recommandations.
6	Gouvernance	Cartographie	L'OSE doit élaborer et mettre à jour la cartographie de chaque système d'information essentiel (SIE) en précisant les applications, les adresses IP, la description fonctionnelle, l'inventaire des dispositifs d'administration et la liste des comptes privilégiés associés au SIE.
7	Protection	Sécurité de l'architecture > Configuration	L'OSE doit installer sur ses systèmes d'information essentiels uniquement les services et équipements indispensables à leur fonctionnement et sécurité, désactiver les services non indispensables, ne connecter que les équipements qu'il gère et analyser le contenu des supports amovibles avant leur utilisation.
8	Protection	Sécurité de l'architecture > Cloisonnement	L'OSE doit cloisonner physiquement ou logiquement ses systèmes d'information essentiels (SIE) ainsi que les sous-systèmes de ces SIE et ne mettre en place que les interconnexions strictement nécessaires pour assurer la sécurité et le bon fonctionnement du SIE, sauf pour les services nécessitant une connexion publique où il doit organiser le SIE en au moins deux sous-systèmes avec des mesures de cloisonnement appropriées pour chaque partie.
9	Protection	Sécurité de l'architecture > Accès distant	L'OSE protège les accès à ses systèmes d'information essentiels, notamment en utilisant des mécanismes cryptographiques conformes aux règles préconisées par l'ANSSI, des authentifications à double facteur et en protégeant les équipements utilisés pour accéder aux SIE par des mécanismes de chiffrement et d'authentification, tout en décrivant ces mécanismes dans le dossier d'homologation de chaque SIE.

	Catégorie	Nom de la règle	Résumé de la règle
10	Protection	Sécurité de l'architecture > Filtrage	L'OSE met en place des mécanismes de filtrage pour limiter la circulation des flux de données inutiles et susceptibles de faciliter les attaques informatiques, en définissant des règles de filtrage pour chaque SIE, en filtrant les flux entrants et sortants des SIE ainsi que les flux entre sous-systèmes des SIE et en établissant et maintenant à jour une liste des règles de filtrage, tout en décrivant ces mécanismes dans le dossier d'homologation de chaque SIE.
11	Protection	Sécurité de l'administration > Comptes d'administration	L'OSE crée des comptes d'administration pour les personnes chargées des opérations d'administration de ses systèmes d'information essentiels, en définissant des règles de gestion et d'attribution de ces comptes en conformité avec la politique de sécurité des réseaux et systèmes d'information, en utilisant le principe du moindre privilège, en utilisant des comptes d'administration pour se connecter aux ressources administrées et en mettant en place des mesures permettant d'assurer la traçabilité et le contrôle des opérations d'administration réalisées sur les ressources qui ne peuvent pas être techniquement administrées à partir d'un compte spécifique.
12	Protection	Sécurité de l'administration > Systèmes d'information d'administration	L'OSE applique des règles strictes aux systèmes d'information utilisés pour l'administration de ses systèmes d'information essentiels, en gérant et configurant exclusivement les ressources matérielles et logicielles de ces systèmes pour les opérations d'administration, en isolant les environnements logiciels, en cloisonnant les flux de données, en connectant les systèmes d'information d'administration aux ressources à administrer via une liaison réseau physique utilisée exclusivement pour les opérations d'administration et en protégeant les flux d'administration par des mécanismes de chiffrement et d'authentification conformes aux règles préconisées par l'ANSSI.
13	Protection	Gestion des identités et accès > Identification	L'OSE crée des comptes individuels pour tous les utilisateurs et les processus automatiques accédant aux ressources de ses systèmes d'information essentiels, et met en place des mesures pour réduire les risques liés à l'utilisation de comptes partagés lorsque la création de comptes individuels n'est pas possible.
14	Protection	Gestion des identités et accès > Authentification	L'OSE protège l'accès aux ressources de ses systèmes d'information essentiels au moyen d'un mécanisme d'authentification impliquant un élément secret et respecte des règles de gestion des éléments secrets d'authentification, et lorsque la ressource ne permet pas techniquement de modifier l'élément secret d'authentification, l'opérateur met en place des mesures de réduction du risque lié à son utilisation.
15	Protection	Gestion des identités et accès > Droits d'accès	L'OSE définit les règles de gestion et d'attribution des droits d'accès aux ressources de ses systèmes d'information essentiels (SIE), en attribuant les droits d'accès uniquement aux utilisateurs ou aux processus automatiques qui en ont strictement le besoin, en révisant les droits d'accès périodiquement, et en établissant et en tenant à jour la liste des comptes privilégiés.
16	Protection	Maintien en conditions de sécurité > Procédure de maintien en conditions de sécurité	L'OSE doit maintenir en conditions de sécurité les ressources de ses systèmes d'information essentiels en fonction de l'évolution des vulnérabilités et des menaces, en installant et en maintenant toutes les ressources matérielles et logicielles dans des versions supportées par leurs fournisseurs ou fabricants et en installant rapidement les mesures correctrices de sécurité lorsqu'il en prend connaissance.
17	Protection	Maintien en conditions de sécurité > Procédure de maintien en conditions de sécurité	L'OSE établit des procédures et mesures de sécurité physique et environnementale pour ses systèmes d'information essentiels, y compris le contrôle du personnel interne et externe, le contrôle d'accès physique et la protection contre les risques environnementaux.
18	Défense	Détection des incidents de sécurité > Détection	L'OSE doit élaborer, mettre à jour et mettre en œuvre une procédure de détection des incidents de sécurité pour ses systèmes d'information essentiels, en se basant sur les exigences du référentiel en matière de détection des incidents de sécurité. Cette procédure doit prévoir des mesures organisationnelles et techniques et permettre la détection d'incidents de sécurité, l'analyse des données issues des capteurs et l'archivage des métadonnées des événements identifiés sur une durée d'au moins six mois.

	Catégorie	Nom de la règle	Résumé de la règle
19	Défense	Détection des incidents de sécurité > Journalisation	L'OSE met en place un système de journalisation sur chaque système d'information essentiel, enregistrant les événements liés à l'authentification des utilisateurs, la gestion des comptes et des droits d'accès, l'accès aux ressources, les modifications des règles de sécurité, ainsi que le fonctionnement du SIE, avec des sources de temps synchronisées pour une durée d'au moins six mois, afin de faciliter la détection d'incidents de sécurité.
20	Défense	Détection des incidents de sécurité > Corrélation et analyse de journaux	L'OSE utilise un système de corrélation et d'analyse de journaux pour détecter les événements susceptibles d'affecter la sécurité de ses systèmes d'information, qui est installé sur un système dédié et exploité conformément aux exigences du référentiel en matière de détection des incidents de sécurité.
21	Défense	Gestion des incidents de sécurité > Réponse aux incidents	L'OSE élabore une procédure de traitement des incidents de sécurité affectant ses systèmes d'information essentiels, et doit mettre en place un système d'information spécifique pour stocker les relevés techniques relatifs aux analyses des incidents, cloisonné vis-à-vis du SIE concerné, tout en se conformant aux exigences du référentiel en matière de réponse aux incidents de sécurité.
22	Défense	Gestion des incidents de sécurité > Traitement des alertes	L'OSE doit mettre en place un service pour recevoir rapidement des informations de l'ANSSI relatives à des incidents, vulnérabilités et menaces, et doit communiquer les coordonnées de ce service à l'Agence. Il doit également mettre en place une procédure pour traiter ces informations et prendre les mesures nécessaires pour protéger ses systèmes d'information essentiels.
23	Résilience des activités	Gestion de crises	L'OSE doit élaborer une procédure de gestion de crise en cas d'incidents de sécurité majeurs, qui prévoit des mesures techniques à appliquer sur les systèmes d'information essentiels tels que la restriction d'accès ou l'isolation du réseau, avec des conditions définies en fonction des contraintes techniques et organisationnelles.

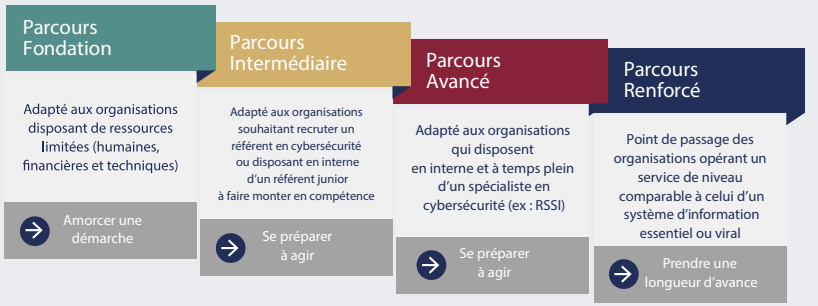
Annexe 5

Éléments complémentaires sur les parcours de cybersécurité de l'ANSSI

Les parcours de cybersécurité proposés par l'ANSSI dans le cadre du volet cybersécurité du plan France Relance ont visé à renforcer la sécurité des systèmes d'information des collectivités territoriales, des établissements de santé et de certains établissements publics, à condition qu'ils disposent d'un système d'information significatif, de ressources humaines disponibles, d'une capacité de cofinancement et d'une réelle motivation s'engager durablement dans le parcours de mise en œuvre.

Les entités bénéficiaires sélectionnées par l'ANSSI pour bénéficier d'un parcours de cybersécurité font d'abord l'objet d'un pré-diagnostic visant à évaluer leur niveau de cybersécurité. Le niveau obtenu permet d'orienter les bénéficiaires vers le parcours au niveau de maturité adapté pour leurs enjeux et leurs besoins.

Les quatre niveaux de maturité des parcours de cybersécurité[222]



[222] *https://www.ssi.gouv.fr/uploads/2021/04/anssi-france_relance-parcours_de_cybersecurite-support_candidats.pdf*

Annexe 6

Liste des briques de sécurité requises pour les différents niveaux de badges

Détail des briques		Graphite	Bronze	Argent	Or	Platine (OIV/OSE)
Données	Système de sauvegarde	X	X	X	X	Obligations légales, réglementaires et techniques spécifiques aux OIV et OSE
	Différents niveaux de cloud/ on-prem			X	X	
Vecteurs	Protection mail	X	X	X	X	
	Protection de la navigation[223]			X	X	
	Stations blanches				X	
	Sas entrée/sortie (diodes, etc.)					
Endpoints	Protection de base des postes utilisateurs (Anti-virus, chiffrement des DD, gestionnaire de mots de passe etc.) mail	X	X	X	X	
	Gestion centralisée des équipements (et des droits), enrôlement, configuration durcie		X	X	X	
	Protection étendue à tous les équipements (téléphone, tablettes, etc.) et remontée de logs				X	
	Système de maintien en conditions de sécurité (installation automatique des mises à jour des correctifs de sécurité, etc.)			X	X	
	EDR (sondes de détection système)				X	

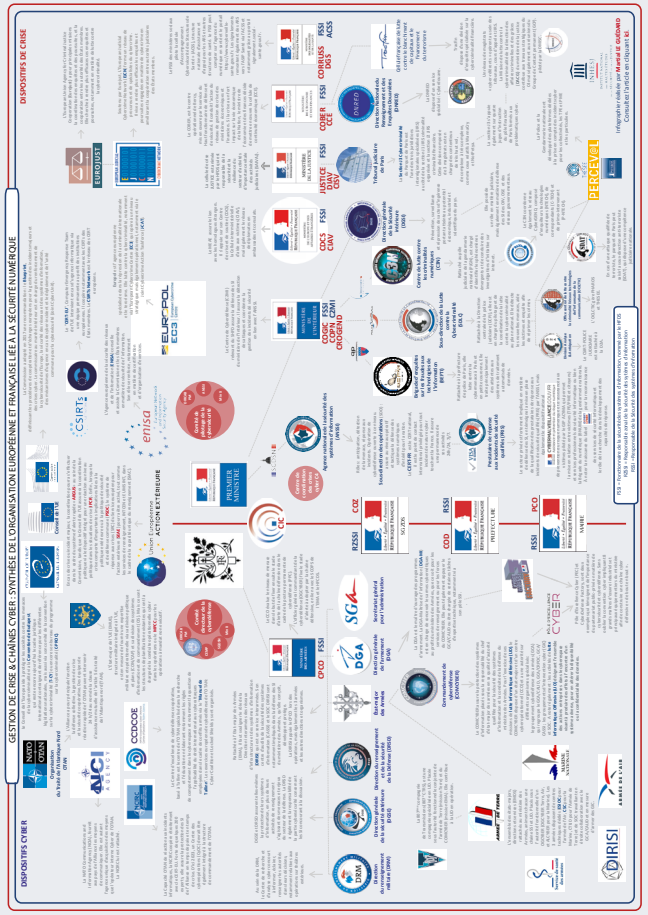
[223] *Avec par exemple, selon une recommandation du BSI allemand, une isolation de chaque page web dans un processus unique.*

Détail des briques		Graphite	Bronze	Argent	Or	Platine (OIV/OSE)
Réseau	Équipements de base pour le filtrage et l'accès distant (pare-feu, VPN, etc.)		X	X	X	
	Segmentation / Cloisonnement[224]		X	X	X	
	Sondes de détection réseau			X	X	
	(Micro) segmentation avancée					
	Dispositifs de sécurité physique et environnementale				X	
Centralisation & Supervision	Gestion des identités et des accès	X	X	X	X	
	Gestion des comptes privilégiés et des systèmes d'administration (moindre privilège, traçabilité, vérification périodique, isolement des systèmes d'administration)			X	X	
	Journalisation des événements (authentifications, accès aux ressources, etc.)		X	X	X	
	Corrélation et analyse de journaux aux fins de détection				X	
	Capacité de réponse à incident dédiée				X	
	Système de traitement des incidents de sécurité (orchestration/ automatisation de la réponse avec un SOAR)				X	
	Dispositif/Service de traitement des alertes de l'ANSSI				X	

[224] *Avec par exemple, selon une recommandation du BSI allemand, une exécution des contenus potentiellement dangereux (pièces jointes des courriels, etc.) dans des mini machines virtuelles (VM pour Virtual Machines en anglais), empêchant la propagation au système complet en cas de présence d'un code malveillant.*

Annexe 7

Organisation de gestion de crise et chaînes cyber en France



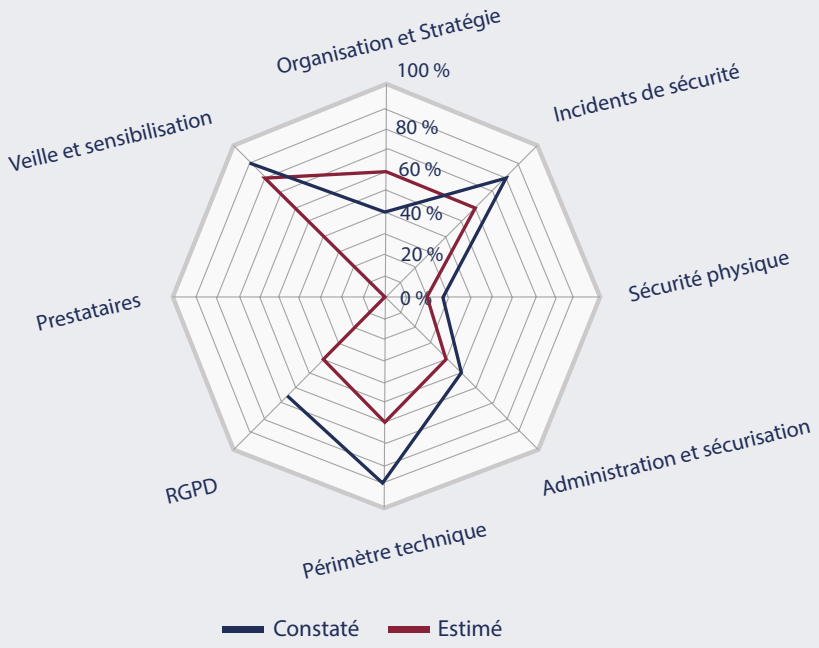
Source : Institut National des Hautes Études de la Sécurité et de la Justice, 2020

Annexe 8

Illustration d'une synthèse des évaluations d'un diagnostic organisationnel et technique (type Di@GoNal), fictif, d'une entreprise, collectivité ou établissement de santé

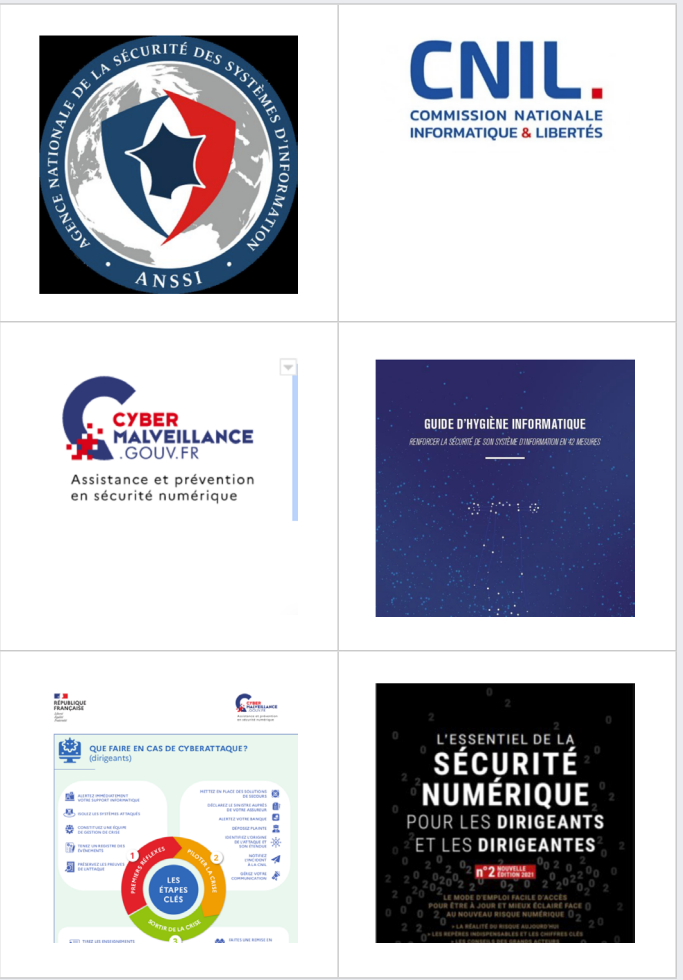
Synthèse des évaluations			
Auto-diagnostic du chef d'entreprise	64 %	63 %	Niveau de vulnérabilité constaté suite à ce pré-diagnostic
Domaine	**Constaté**	**Estimé**	**Perception du risque**
Organisation et stratégie	42 %	60 %	Risque légèrement surévalué
Veille et sensibilisation	89 %	80 %	Risque bien évalué
Prestataires	N/A	0 %	
RGPD	64 %	40 %	Risque sous évalué Sensibilisation à mener
Périmètre technique	88 %	60 %	Risque sous évalué Sensibilisation à mener
Administration et sécurisation	49 %	40 %	Risque bien évalué
Sécurité physique	27 %	20 %	Risque bien évalué
Incidents de sécurité	77 %	60 %	Risque sous évalué Sensibilisation à mener

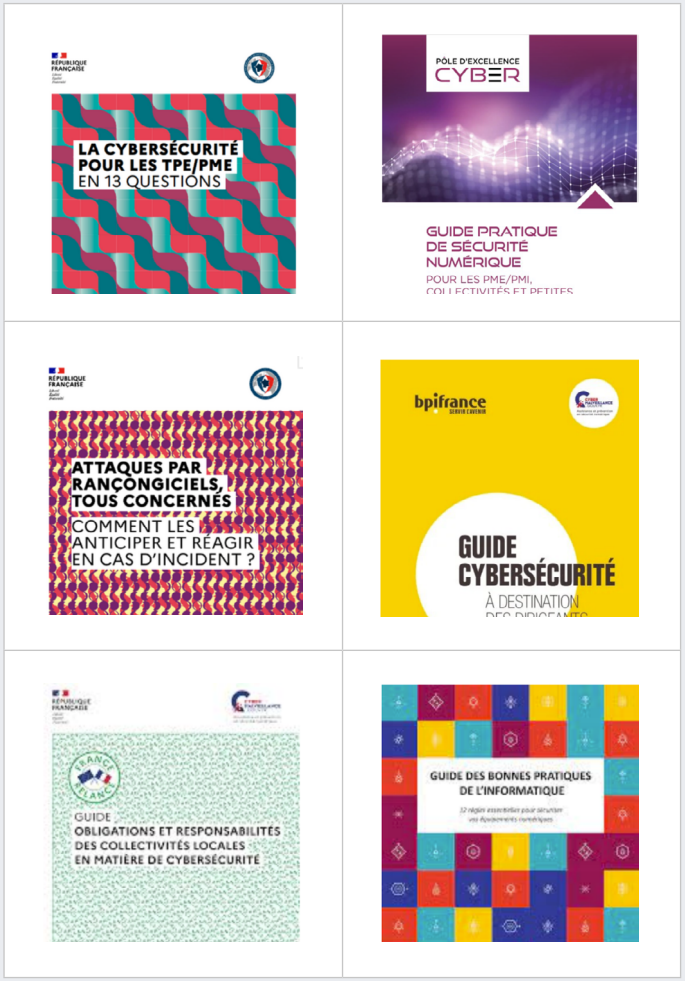
Synthèse des évaluations



Annexe 9

Principales ressources utiles pour sécuriser sa structure





Remerciements

L'Institut Montaigne remercie l'ensemble des personnes ayant contribué à l'élaboration de ce travail :

PRÉSIDENTS DU GROUPE DE TRAVAIL

- **Gérôme Billois,** associé en charge des sujets cybersécurité et confiance numérique au sein du cabinet Wavestone
- **Olivier Vallet,** président-directeur général de Docaposte

MEMBRES DU GROUPE DE TRAVAIL

- **Jean-Baptiste Fontenille,** Expert résident, Institut Montaigne (rapporteur)
- **Godefroy Galas,** chargé de mission à la sous-direction opérations de l'ANSSI, ingénieur des mines (rapporteur)
- **Jean-Jacques Latour,** directeur expertise cybersécurité de Cybermalveillance.gouv.fr
- **William Lecat,** directeur d'investissements chez Auriga Cyber Ventures et ancien coordinateur de la stratégie nationale d'accélération pour la cybersécurité
- **Guillaume Poupard,** directeur général adjoint de Docaposte, ancien directeur général de l'ANSSI
- **Milo Rignell,** responsable de projets et expert résident - Nouvelles technologies au sein de l'Institut Montaigne

LE GROUPE DE TRAVAIL REMERCIE ÉGALEMENT LES PERSONNES SUIVANTES POUR LEUR AIDE PRÉCIEUSE :

- **Marc Bothorel**, Référent cybersécurité de la Commission numérique, CPME
- **Tom David**, assistant chargé d'études à l'Institut Montaigne
- **David Tortel**, associé, Deloitte France et Afrique Francophone

PERSONNES AUDITIONNÉES

- **Laurent Amsel**, *Group Chief information security officer*, Carrefour
- **José Araujo**, *Group chief technology officer*, Orange Cyber Defense
- **Benoît Waltregny**, *Chief Corporate & Legal Officer*, Lloyd's Europe
- **Vivien Bilquez**, *Global Cyber Risk Engineer*, Zurich Resilience Services (ZRS)
- **Dominique Bogé**, chef du département prévention et confiance numérique, Gendarmerie nationale
- **Yann Bonnet**, Directeur général délégué, Campus Cyber
- **Marc Bothorel**, Référent cybersécurité de la Commission numérique, CPME
- **Remi Bottin**, Directeur Synergies & Développement, Bessé
- **Amélie Breitburd**, CEO, Lloyds Europe
- **Etienne Busnel**, Directeur des Systèmes d'Information, Bessé
- **Lucas Buthion**, *Public affairs Manager*, Iliad
- **Guillaume Cali**, Référent cybersécurité de la Commission numérique, Direction de la Stratégie et du Développement
- **Pierre Cejka**, Relations Institutionnelles & Médias, Bpifrance
- **Laurent Celerier**, *Executive vice-president* "Central Europe & International Business", Orange Cyberdéfense
- **Thomas Chast**, responsable du pôle communication et pilotage du RECYM (Réseau des Experts CyberMenaces), DCPJ
- **Elodie Chaudron**, directrice du programme CaRE - Copilotage Task Force Cyber, Agence du numérique en santé
- **Delphine Chevallier**, Fondatrice, Thalia Neomedia
- **Bénédicte Constans**, Directrice de la Communication et des Affaires publiques, Zurich Insurance France
- **Valéry Dajon,** Dirigeant SERVALY / CEO et cofondateur People Booster, Servaly
- **Benoit De Corn**, Directeur stratégie Télécom & Digital, La Poste
- **Jean-Noël De Galzain**, Président d'Hexatrust, PDG de Wallix Group et Pilote du Projet Cybersécurité du CSF
- **Luc Declerck**, *Managing Director*, Board of Cyber
- **François Dégez**, Chef de la division coordination territoriale, Agence nationale de la sécurité des systèmes d'information
- **Pierre Deheunynck,** Directeur Général de Ricol-Lasteyrie et Président de France compétences
- **Christophe Delcamp**, Directeur, France assureurs
- **Maxime Donadille**, Conseiller technologies d'avenir, espaces immersifs et cybersécurité, Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique
- **Thierry Dor**, *Partner*, Gide Loyrette Nouel
- **Valentin Durand**, *Country Digital Acceleration Program* - France Lead, Cisco
- **François Esnol-Feugeas**, Vice-Président de l'ACN et CEO Oxibox
- **Jean-Marc Esvant**, Directeur général adjoint, Verlingue
- **Jérôme Fehrenbach**, Directeur général, Conseil supérieur du notariat
- **Arnaud Fournier**, *Co-Founder & CEO*, Bastion
- **Jacques Frénéhard**, Président, Groupe Frénéhard et Michaux
- **Thomas Fressin**, Maître de conférences associé en informatique, Université Gustave Eiffel
- **Eric Freyssinet,** Général, Directeur scientifique GN - Cabinet DGGN, Gendarmerie nationale
- **Tristan Fulchiron**, Conseiller transformation numérique du Ministre de l'Intérieur et des Outre-mer, Ministère de l'Intérieur et des Outre-mer
- **Frédéric Géraud**, *Head of Government Affairs & Public Policy*, Google
- **Dimitri Grygowski**, *Governement Affairs Manager*, Cisco
- **Quentin Guérineau**, Chef de bureau, Sous-direction des assurances

(Direction générale du Trésor)
- **Jonathan Guiffard**, Expert résident, Institut Montaigne
- **Valentin Heude**, Responsable de projets, Transports Vallée
- **Christophe Husson,** Général, Commandant en second de la gendarmerie dans le Cyberespace (COMCYBERGEND)
- **Georges-Axel Jaloyan**, Chercheur en rétro-ingénierie de cybersécurité, Commissariat à l'énergie atomique
- **Yoann Kassianides**, Délégué général, Alliance pour la confiance numérique
- **Florent Kirchner**, Coordinateur de la stratégie nationale pour la cybersécurité, Secrétariat général pour l'investissement
- **Marwan Lahoud**, directeur général délégué de Tikehau et président du Private Equity de Tikehau
- **Martin Landais**, Sous-directeur des assurances, Direction générale du
- Trésor (Ministère de l'économie)
- **Marie-Liane Lekpeli**, Directrice de projets numérique responsable et sécurité, DGE MINECO
- **Xavier Leonetti**, Magistrat
- **Olivier Ligneul**, *Group Chief Information Security Officer*, EDF
- **Aurélien Lopez-Liguori**, Député, Assemblée nationale
- **Christophe Madec**, Directeur de clientèle - Grandes entreprises et Expert Cyber/Fraude, Bessé
- **Jean-Pierre Marbaix**, Prévention IARD, AXA
- **Eric Marlière-Albrecht**, Commandant de police, chef par intérim du Pôle du Renseignement Cyber de l'OCLCTIC (DCPJ)
- **Arnaud Martin**, *Chief Information Security Officer*, Caisse des Dépôts
- **Gwenaelle Martinet**, Conseillère France Relance, Agence nationale de la sécurité des systèmes d'information (ANSSI)
- **Christophe Meganck**, Délégué Général, club ETI Normandie
- **Gérard Messanvi**, Délégué général adjoint, METI
- **Thiébaut Meyer**, Director, Office of the CISO, Google
- **Anne Mimin**, Directrice adjointe chargée de la stratégie territoriale, Ugap

- **Michael Monerau**, CEO & Fondateur, Qontrol
- **Bertrand Monnet**, Professeur, EDHEC
- **Alexandre Montay**, Délégué général, METI
- **Sébastien Morey**, Responsable du CSIRT Bourgogne- Franche-Comté et de l'ARNIA Cybersécurité
- **Marc Mossé**, Avocat aux Barreaux de Paris et de Bruxelles, Senior Counsel, August & Debouzy
- **Denis Mottier**, Chargé de mission, Association des maires de France et des présidents d'intercommunalité (AMF)
- **Jérôme Normand**, Economiste, CPME
- **Olivier Panis**, Senior Vice President FIG, Moody's
- **Benoît Parizet**, *Chief digital officer*, Caisse des dépôts et consignations
- **Stefan Recher**, *Executive VP*, Innovation, Digital/IT & Advisory, Bourbon
- **Annick Rimlinger**, Directrice Sûreté & Sécurité, Cyber et Data Protection, Aéma Groupe
- **Jean-Louis Rougier**, Professeur, Télécom Paris
- **Frédéric Sardain**, *Partner - IP*, Tech & Data, Jeantet
- **Sophie Scemla**, *Partner*, Gide Loyrette Nouel
- **Phillipe Steing,** Associé-Partner, Ricol Lasteyrie
- **Camille Stoclin-Mille**, Administratrice en charge des relations avec les institutions, Conseil supérieur du notariat
- **Vincent Strubel**, Directeur Général, Agence nationale de la sécurité des systèmes d'information (ANSSI)
- **Vincent Trel**, Président, APSSIS
- **Michel Van Den Berghe**, Président, Campus Cyber
- **Arnaud Vandesmet**, Directeur de la sécurité des systèmes d'information et de la protection des données, Ramsay Santé
- **Jules Veyrat**, Président et co-fondateur, Stoïk
- **Barnabé Watin-Augouard**, Chef de division du COMCYBERGEND, Gendarmerie nationale
- **Marc Watin-Augouard**, Fondateur du Forum international de la cybersécurité (FIC), Général d'armée de la Gendarmerie nationale

L'INSTITUT MONTAIGNE REMERCIE ÉGALEMENT POUR LEUR AIDE PRÉCIEUSE :

- **Le Mouvement des entreprises de taille intermédiaire (METI)**
- **Le groupement de gendarmerie départementale du Calvados**
- **Le CSIRT de la région Bourgogne-Franche-Comté**

Les opinions exprimées dans ce rapport n'engagent ni les personnes précédemment citées ni les institutions qu'elles représentent.

Retrouvez nos autres notes et rapports sur les sujets tech et innovation :

- **Mobiliser et former les talents du numérique** (mai 2023)
- **Investir l'IA sûre et digne de confiance : un impératif européen, une opportunité française** (avril 2023)
- **Géopolitique et technologie : le tournant de la stratégie européenne** (mars 2022)
- **Innovation française : nos incroyables talents** (octobre 2021)
- **Fintech chinoise : l'heure de la reprise en main** (avril 2021)
- **Enseignement supérieur et recherche : il est temps d'agir !** (avril 2021)
- **Cybermenace : avis de tempête** (novembre 2018)

L'ensemble de nos travaux et publications
est disponible sur notre site institutmontaigne.org

INSTITUT Montaigne

Président

- **Henri de Castries**, président, Institut Montaigne

Membres

- **David Azéma**, associé, Perella Weinberg Partners
- **Emmanuelle Barbara**, *Senior Partner*, August Debouzy
- **Marguerite Bérard**, directrice des Réseaux France, BNP Paribas
- **Jean-Pierre Clamadieu**, président du Conseil d'Administration, ENGIE
- **Paul Hermelin**, président du Conseil d'administration, Capgemini
- **Marwan Lahoud**, président, Ace Capital Partners
- **Natalie Rastoin**, présidente, Polytane ; Senior Advisor, WPP
- **René Ricol**, président, Ricol Lasteyrie
- **Jean-Dominique Senard**, président du Conseil d'administration, Groupe Renault
- **Arnaud Vaissié**, président-directeur général, International SOS
- **Natacha Valla**, économiste ; doyenne de l'École de Management et d'Innovation, Sciences Po
- **Florence Verzelen**, directrice générale adjointe, Dassault Systèmes
- **Philippe Wahl**, président-directeur général, Groupe La Poste

Président d'honneur

- **Claude Bébéar**, fondateur et président d'honneur, AXA

L'Institut Montaigne vous propose de contribuer à la réflexion sur ces enjeux afin d'élaborer collégialement des propositions au service de l'intérêt général.

Les adhérents

INSTITUT Montaigne

ABB France
Abbvie
Accenture
Accuracy
Adeo
ADIT
Air France - KLM
Air Liquide
Airbus
Allen & Overy
Allianz
Amazon
Amber Capital
Amundi
Antidox
Antin Infrastructure Partners
Archery Strategy Consulting
Archimed
Ardian
Arquus
Astrazeneca
August Debouzy
Avril
AXA
Bain & Company France
Baker & Mckenzie
Bearingpoint
Bessé
BG Group
BNP Paribas
Bolloré
Bona Fidé
Bouygues
Brousse Vergez
Brunswick
Capgemini
Capital Group
CAREIT
Carrefour
Casino
Chubb
CIS
Cisco Systems France
Clifford Chance
Club Top 20
CMA CGM
CNP Assurances
Cohen Amir-Aslani
Compagnie Plastic Omnium
Conseil supérieur du notariat
Crédit Agricole
D'angelin &Co.Ltd
Dassault Systèmes
De Pardieu Brocas Maffei
Doctolib
ECL Group
Edenred
EDF
EDHEC Business School
Egis
Ekimetrics France
Enedis
Engie
EQT
ESL & Network
Ethique & Développement
Eurogroup Consulting
FGS Global Europe
Fives
Getlink
Gide Loyrette Nouel
Google
Groupama
Groupe Bel
Groupe M6
Groupe Orange
Hameur Et Cie
Henner
Hitachi Energy France
HSBC Continental Europe
IBM France
IFPASS
Inkarn
Institut Mérieux
International SOS
Interparfums
Intuitive Surgical
Ionis Éducation Group
iQo
ISRP
Jeantet Associés
Jolt Capital
Kantar Public
Katalyse
Kea & Partners
Kearney
Kedge Business School
KKR
KPMG S.A.
Kyndryl
La Banque Postale
La Compagnie Fruitière
Linedata Services
Lloyds Europe
L'Oréal
Loxam
LVMH - Moët-Hennessy - Louis Vuitton
M.Charraire
MACSF
MAIF
Malakoff Humanis
Mazars
Média-Participations
Mediobanca
Mercer
Meridiam
Michelin
MicroPort CRM
Microsoft France
Mitsubishi France S.A.S
Moelis & Company
Moody's France
Morgan Stanley
Natixis
Natural Grass
Naval Group
Nestlé
OCIRP
ODDO BHF
Oliver Wyman
Ondra Partners
onepoint
Onet
Optigestion
Orano
PAI Partners
Pelham Media
Pergamon
Prodware
PwC France & Maghreb
Raise
RATP
RELX Group
Renault
Rexel
Ricol Lasteyrie
Rivolier
Roche
Rokos Capital Management
Roland Berger
Rothschild & Co
RTE
Safran
Sanofi
SAP France
Schneider Electric
Servier
SGS
SIER Constructeur
SNCF
SNCF Réseau
SNEF
Sodexo
SPVIE
SUEZ
Taste
Tecnet Participations SARL
Teneo
The Boston Consulting Group
Tilder
Tofane
TotalEnergies
UBS France
Unibail-Rodamco
Veolia
Verlingue
VINCI
Vivendi
Wakam
Wavestone
Wendel
White & Case
Willis Towers Watson France
Zurich

Institut Montaigne
59 rue La Boétie, 75008 Paris
Tél. +33 (0)1 53 89 05 60
institutmontaigne.org

Imprimé en France
Dépôt légal : juin 2023
ISSN : 1771-6764

L'intensification de la cybercriminalité et le développement de directives de cybersécurité appellent une prise de conscience rapide et massive des acteurs diffus du territoire, petites et moyennes entreprises, établissements de santé et collectivités, diversement engagés jusqu'à présent dans leur protection face aux menaces cyber. Pourtant, il s'agit là d'un enjeu majeur de résilience économique et sociale, la moitié des PME attaquées faisant faillite après une cyberattaque.

L'État est un acteur compétent mais ses actions ne sont pas nécessairement coordonnées aux échelles appropriées des structures à protéger – régions, départements, communes. Et cette coordination doit non seulement s'appliquer à prévenir les cyberattaques, elle doit aussi traiter au mieux leur remédiation et leur répression.

Ainsi, il apparaît nécessaire de créer les conditions d'un passage à l'échelle pour protéger plus exhaustivement le territoire. À partir d'une analyse collégiale et de terrain, conduite en partenariat avec La Gendarmerie nationale, le METI et le groupe La Poste, le rapport propose une méthode simple et rapidement opérationnelle fondée sur les solutions et acteurs existants dans une logique incrémentale, pragmatique et facilement implémentable.

La conviction des professionnels du secteur est qu'il suffit parfois de peu pour améliorer la sécurité des structures, pour autant que celles-ci en comprennent l'utilité et en acceptent les modalités pratiques. Le numérique irriguant désormais tous nos usages, la sécurité doit devenir un réflexe naturel, comme le port de la ceinture de sécurité dans les voitures ou la fermeture de la porte d'entrée de sa maison : un comportement de bon sens que personne ne remet en cause.

Les conditions clés pour un passage à l'échelle effectif et réussi reposent essentiellement sur l'articulation des efforts des différents acteurs nationaux et locaux en temps réel et la mobilisation rapide des moyens identifiés.

10 €
ISSN : 1771-6764
RAP2306-02