<CAMPUS CYBER>

RAPPORT MISSION PME & CYBERSÉCURITÉ

Le Président du Campus Cyber, Michel Van den Berghe, et son équipe : Yann Bonnet, Directeur général délégué du Campus Cyber ; Lucile Briolat, Chargée de projets écosystème et international ; Magali Marques, Directrice de Cabinet ; Mathilde Pareau, Alternante veille et écosystème

<Synthèse>

Bien que notre dépendance aux outils numériques soit en constante hausse, la pandémie du COVID a marqué un tournant en termes d'exposition au risque numérique. Le virage forcé effectué vers un monde connecté a augmenté les surfaces d'attaque possibles. D'après le panorama de la menace de l'ANSSI, les rançongiciels ont été multipliés par 4 entre 2019 et 2020[1]. La menace est protéiforme, croissante et ne cesse de se renouveler. C'est pourquoi, en 2022, pour la première fois, la cybersécurité a été classée dans le TOP 10 des risques business par le Forum économique mondial[2].

Les conséquences d'une attaque cyber sont multiples : économiques, sociales, humaines, etc. Car si le coût d'une attaque s'élève de plusieurs dizaines de milliers à plusieurs millions d'euros, elle a également un impact réel sur le quotidien des individus : arrêt d'un hôpital, pertes de données personnelles, stress élevé, etc. La dernière attaque contre la collectivité de la Martinique au mois de mai 2023 s'est traduite, par exemple, par une incapacité à verser les prestations sociales pendant plusieurs semaines. Trois mois plus tard, les systèmes ne sont toujours pas rétablis. Il est donc nécessaire de protéger les systèmes en anticipant le risque et identifiant les faiblesses de la structure informatique.

Dans ce contexte, dépendantes aux technologies numériques mais peu préparées à faire face aux risques, les plus petites entreprises sont des acteurs fragiles. En effet, 56% des PME ont connu au moins un incident cyber en 2021[3] et 50% des PME font faillite dans les 18 mois suivant une attaque[4]. La cybersécurité des TPE/PME/ETI[5] constitue donc un réel risque pour notre santé économique, d'autant que les PME représentent plus de 99% du tissu économique français, soit plus de 4 millions d'entreprises[6].

La cybersécurité est une préoccupation des grands groupes depuis plusieurs années. L'ANSSI a noté pour la première fois en 2022 une diminution d'attaque réussie vers ces acteurs et un détournement de la menace vers les PME, moins bien protégées[7]. Cela s'explique notamment par : un manque de moyens financiers, de temps et de connaissance sur l'état réel de la menace mais également une difficulté à s'orienter vers les solutions adaptées au sein d'un marché foisonnant et usant d'un vocabulaire parfois complexe. Ainsi, la cybersécurité doit permettre aux PME d'assurer la continuité de leurs activités, sans devenir une difficulté technique.

Face à ce constat, les législations françaises et européennes se renforcent pour inciter et obliger à la sécurisation des PME. D'ici octobre 2024, la directive européenne NIS2 sera transposée en droit français : elle vise à renforcer la cybersécurité des acteurs les plus faibles en responsabilisant l'ensemble de la chaine d'approvisionnement. Dans les prochains mois, les PME vont donc devoir mettre en place des solutions de cybersécurité pour être en conformité avec la législation. Par ailleurs, le développement en cours d'une offre d'assurance cyber va nécessairement s'accompagner d'une définition des niveaux minimum de sécurité informatique à atteindre pour y souscrire.

Concernant les politiques françaises, ces dernières se sont concentrées sur la protection des acteurs sensibles et acteurs publics. Le GIP ACYMA et le développement en cours des CSIRT régionaux représentent la possibilité pour les PME de disposer d'interlocuteurs privilégiés en cas d'attaque. Néanmoins, il est nécessaire d'accentuer ces politiques pour passer à l'échelle rapidement en termes de sécurisation des PME, notamment en clarifiant les besoins et les offres du marché adaptés au niveau de maturité et au secteur d'activité de chaque PME.

De nombreux acteurs se sont d'ores et déjà organisés pour apporter une réponse à cet enjeu : guides de bonnes pratiques et solutions de sécurisation des systèmes d'information existent, au niveau privé comme public. Néanmoins, cette offre foisonnante est parfois désorganisée et souvent complexe à appréhender par des PME novices, d'autant qu'un vocabulaire technique est souvent utilisé. Une réelle coordination entre les acteurs et activités existantes est donc à trouver pour passer de la prise de conscience du risque en cours (75% des dirigeants ont conscience du risque[8]) à la mise en place concrète d'outils de sécurité numérique.

Il est urgent d'agir collectivement car il existe un risque de crise majeure. Une attaque massive des PME constituerait un blocage sans précédent des activités économiques et sociales du pays.

Michel Van den Berghe, Président du Campus Cyber, a donc été missionné en décembre 2022 par le Ministre Jean-Noël Barrot pour la conduite d'un plan de recommandations pour une plus grande sécurisation des TPE, PME et ETI françaises[9]. Cette mission s'est appuyée pour produire ce rapport sur des auditions des acteurs publics et privés[10], des questionnaires recensant[11] les dispositifs existants chez les acteurs publics et privés[12], des focus groupe PME, des restitutions groupées et une analyse des modèles mis en place dans 7 pays[13].

[1] Panorama de l'état de la menace de l'ANSSI 2020, CERTFR-2021-CTI-001.pdf (ssi.gouv.fr)
[2] The global risks report 2022, WEF_The_Global_Risks_Report_2022.pdf (weforum.org)
[3] Rapport du Sénat sur la cybersécurité des entreprises 2021, Modèle pour la frappe des Rapports Parlementaires (senat.fr)
[4] Jean-Noël Barrot, ministre délégué chargé de la transition numérique et des télécommunications
[5] Définitions selon l'art. 51 de la loi de modernisation de l'économie : « Une microentreprise est une entreprise dont l'effectif est inférieur à 10 personnes et dont le chiffre d'affaires ou le total du bilan annuel n'excède pas 2 millions d'euros. Une PME est une entreprise dont l'effectif est inférieur à 250 personnes et dont le chiffre d'affaires annuel n'excède pas 50 millions d'euros ou dont le total de bilan n'excède pas 43 millions d'euros. Une ETI, entreprise de taille intermédiaire, est une entreprise qui n'appartient pas à la catégorie des PME, dont l'effectif est inférieur à 5000 personnes et dont le chiffre d'affaires annuel n'excède pas 1 500 millions d'euros ou dont le total de bilan n'excède pas 2 000 millions d'euros. »
Utilisation du termes PME pour désigner l'ensemble dans le rapport
[6] INSEE, les entreprises en France, édition 2021, Catégories d'entreprises – Les entreprises en France | Insee
[7] Panorama de l'état de la menace de l'ANSSI 2022, CERTFR-2023-CTI-001.pdf (ssi.gouv.fr)
[8] Etude IPSOS pour cisco, Etude Cisco : Le risque cyber est perçu comme faible voire inexistant pour un quart des entreprises françaises - Cisco News The EMEA Network
[9] Voir annexes « Lettre de mission »
[10] Voir annexes « Liste des personnes et entités entendues »
[11] Voir annexes « Synthèse des réponses au questionnaire »
[12] Voir annexes « Cartographie (non exhaustive) des dispositifs »
[13] Voir annexes « Synthèse des questionnaires des services économiques des ambassades »

<Recommandations>

Rendre plus lisible les premières étapes clés pour amorcer puis renforcer la sécurisation des PME.

1

LA PROBLÉMATIQUE

Bien qu'une multitude de diagnostics existe, leur réalisation est insuffisamment suivie par la mise en place de mesures par les PME. Cela est dû à leur complexité et technicité, souvent inadaptées au niveau de maturité des entreprises qui les réalisent.

LA SOLUTION

Nous proposons de rendre plus lisibles les dispositifs de diagnostics. Il existe un consensus sur, d'une part le besoin d'harmoniser les travaux de diagnostics et, d'autre part, le nécessaire accompagnement des entreprises dans le passage à l'action une fois le diagnostic réalisé.

<Pour les PME les moins matures, étendre l'expérimentation MonAideCyber portée par l'ANSSI>

En cours en Nouvelle-Aquitaine, d'autres régions pourraient tester ce dispositif comme l'Ile-de-France via l'EDIH CYBIAH, la Bretagne ou encore les Haut-de-France via le Campus Cyber Territorial. L'initiative doit être généralisée au niveau national.

MON AIDE CYBER

La startup d'Etat de l'ANSSI « MonAideCyber » expérimente un dispositif avant son déploiement fin 2023.

Il s'agit d'un diagnostic cyber (une quarantaine de questions) rapide destiné aux entités publiques et privées faiblement matures dites « sensibilisées au cyber mais souhaitant structurer leur action ».

Ce diagnostic est réalisé par des « aidants cyber » de confiance, sélectionnés, formés et accompagnés par l'ANSSI (gendarmerie, police, douanes, associations sectorielles) et bientôt via le réseau des Campus Cyber en région.

Il propose en sortie 6 recommandations priorisées à réaliser en 6 mois avec un accompagnement possible durant ces 6 mois afin que ces actions soient bien mises en œuvre.

<Pour les PME plus matures, la DGE et l'ANSSI doivent publier un référentiel adapté. L'accompagnement doit être réalisé par des acteurs privés, à l'exception faite des dispositifs financés par l'Etat>

Utilisée pour estimer la maturité cyber de plus de 900 collectivités territoriales, les « parcours » de l'ANSSI est une méthode pouvant être déclinée pour les PME. Ce référentiel doit devenir un commun accessible à tous les acteurs publics et privés, y compris à des fins commerciales.

LES « PARCOURS DE L'ANSSI »

A destination des collectivités territoriales, ce parcours permet de définir le niveau de maturité et les actions à mettre en place rapidement.

Condition préalable : avoir une structure informatique et une personne en charge de sa sécurisation.

Processus développé en plusieurs étapes : audit, modules de sensibilisation des responsables, définition d'un plan d'action et des moyens humains associés. Ce processus permet de responsabiliser les équipes tout en étant directif dans la mise en place des actions de sécurisation des systèmes d'information.

<Recommandations>

Créer une place de marché nationale de prévention au risque cyber pour les PME.

2

Centraliser les outils et services adaptés à la taille, localisation et secteur d'activité de la PME.

LA PROBLÉMATIQUE

Bien que les PME aient de plus en plus conscience du risque cyber, elles ne savent pas vers qui s'orienter pour leurs démarches de sécurisation. En parallèle, les acteurs de l'écosystème qui proposent des dispositifs de sécurisation ont des difficultés à adresser le vaste marché que représentent les PME.

LA SOLUTION

Nous proposons **la mise en place d'une place de marché centralisée nationale** recensant des offres packagées pour permettre l'orientation des PME vers les outils adaptés en fonction de leur taille, niveau de maturité, localisation et secteur d'activité. De par son rôle de lieu totem de l'écosystème, le Campus Cyber est le bon acteur pour porter cette plateforme.

<Points clefs à mettre en avant>

</> **Diagnostics et dispositifs de scoring, y compris financiers, pour aider les dirigeants à prendre conscience du risque.**

</> **Offres proposées par des acteurs publics et privés** (Sélections et labellisation des solutions selon des critères transparents ainsi qu'un processus de test par des acteurs de l'écosystème).

</> **Services disponibles en termes de sensibilisation et de réaction, notamment cybermalveillance.gouv.fr**

</> **Formation en ligne (MOOC) à destination des salariés et dirigeants.**

</> **Dispositifs d'obtention d'un label ou d'un badge, pouvant par exemple faciliter la souscription à une assurance cyber, visant à inciter les PME à se sécuriser.** (Ce concept d'attribution de badge existe dans le dispositif Boost Aerospace. Il est une recommandation du rapport de l'Institut Montaigne Cybersécurité, passons à l'échelle. Cela permettrait d'aider les structures à préciser leur objectif en termes de cybersécurité. Une telle initiative aurait beaucoup de sens si elle était réalisée au niveau européen).

</> **Dispositifs d'entrainement à la gestion d'une crise cyber majeure en impliquant des PME au niveau des régions, via le réseau associatif local**

Pour réaliser cette plateforme, nous recommandons une approche UX design (expérience utilisateur) visant à simplifier son usage pour le grand public. Cette plateforme serait à coconstruire avec les PME pour définir la boite à outils nécessaire à leur sécurisation.

<Recommandations>

Créer une campagne de prévention cyber et un kit de sensibilisation clé en main.

3

Sensibiliser et prévenir largement les 4 millions de PME

LA PROBLÉMATIQUE

Bien que les PME aient de plus en plus conscience du risque cyber, il est nécessaire de poursuivre et d'intensifier collectivement les actions afin que l'ensemble des PME françaises passent à l'action.

LA SOLUTION

Nous proposons d'utiliser deux canaux de communication de prédilection pour atteindre le plus grand nombre :

<Sensibiliser largement les PME en organisant une campagne de prévention cyber 360° sur le modèle des spots TV dédiés à la prévention routière>

Cette campagne serait coconstruite entre ACYMA et Campus Cyber. Elle redirigerait les PME vers la plateforme cybermalveillance.gouv.fr, guichet unique de lutte contre les cyber malveillances, ainsi que le projet de future plateforme «17 cyber», portée par le ministère de l'Intérieur. Elle redirigerait également vers la place de marché nationale de prévention. Sa diffusion sur les réseaux sociaux utilisés par les chefs d'entreprise, comme LinkedIn, augmenterait son impact.

<S'appuyer sur les interlocuteurs de proximité et de confiance des PME, dits « connecteurs », afin de rapidement passer à l'échelle>

La production d'un kit de communication partagé et actualisé permettrait la diffusion d'un discours harmonisé et compréhensible vers les PME par ces acteurs clefs afin de renforcer la sensibilisation et prévention. L'objectif serait notamment de rediriger vers la place de marché.

Exemples de « connecteurs » : banques, assurances, La Poste, opérateurs de télécommunications, experts comptables, Campus Cyber Territorial, les CSIRT, Experts Cyber, communauté des aidants de MonAideCyber, associations professionnelles, associations locales, intégrateurs locaux, grands groupes pour les chaines d'approvisionnement, conseillers numériques, forces de l'ordre (dont la formation doit être renforcée).

Le réseau des Campus Cyber territoriaux aura un rôle particulier dans l'activation des connecteurs.

annexes

Lettre de mission

MINISTÈRE CHARGÉ DE LA TRANSITION NUMÉRIQUE ET DES TÉLÉCOMMUNICATIONS

Liberté
Égalité
Fraternité

JEAN-NOËL BARROT

Paris, le 15 DEC. 2022

Ministre délégué

Nos références : MEFI-A22-21188

Monsieur le Président du Campus Cyber, cher Michel,

Le Président de la République vous a confié en 2019 la mission de créer le lieu de référence de la cybersécurité en France. Ce lieu, le Campus Cyber, a été inauguré par Bruno Le Maire, Ministre de l'Economie et des Finances, en février 2022. Réel succès, il est la preuve concrète de la volonté de l'écosystème de la cybersécurité de se fédérer.

Cette structuration de notre écosystème est un impératif majeur dans un contexte d'accroissement soutenu de la menace cyber, qui concerne désormais tous les pans de notre société et de notre économie. Chaque jour en France, 7 incidents contre des systèmes d'informations sensibles sont notifiés à l'ANSSI et 500 victimes (particuliers, entreprises, collectivités) en moyenne font une demande d'assistance sur la plateforme Cybermalveillance.gouv.fr

Face à la multiplication des cyberattaques, le Gouvernement mobilise différents leviers afin de protéger nos concitoyens et entreprises et leur permettre de tirer pleinement parti des opportunités offertes par les nouvelles technologies dans un espace numérique le plus sûr et sécurisé possible.

Pour ce faire, l'Etat s'appuie en particulier sur l'ANSSI et les autres administrations pour la sécurisation et la cyberdéfense des cibles sensibles, ainsi que sur les actions de sensibilisation et d'assistance aux victimes que conduit le groupement d'intérêt public ACYMA au bénéfice des autres acteurs de la société. Il met également en œuvre des dispositifs de soutien direct à l'élévation du niveau de cybersécurité des organismes publics et déploie une stratégie d'accélération dotée de 720 millions d'euros de fonds publics qui vise à accompagner le développement de la filière française de la cybersécurité.

Monsieur Michel VAN DEN BERGHE
Président du Campus Cyber
5-7, rue Bellini
92 800 PUTEAUX

Notre pays possède de nombreux atouts pour faire face à la progression de la menace et renforcer sa souveraineté numérique. Il peut s'appuyer non seulement sur de grands groupes industriels mais également sur un écosystème de startups innovantes, des structures de formation et de recherche, des organismes publics. Tous sont désormais réunis au sein du Campus Cyber, véritable centre opérationnel, permettant à plus de 3 000 experts de travailler ensemble pour améliorer notre résilience collective face au risque cyber et mieux protéger la Nation.

Si l'action collective engagée depuis 2017 produit des résultats très encourageants, elle se heurte également à certaines limites qui doivent être surmontées pour porter le niveau général de maturité cyber de notre pays à un niveau satisfaisant. Un des axes d'amélioration identifié porte spécifiquement sur une meilleure prise en compte des problématiques de cybersécurité par notre tissu économique d'ETI, de TPE-PME et de jeunes entreprises innovantes. A l'inverse des grands groupes, les dirigeants et collaborateurs de ces entreprises restent bien souvent éloignés des enjeux de cybersécurité, faute d'une culture et vision stratégique suffisamment développées, de moyens ou d'expertise interne.

C'est la raison pour laquelle j'ai annoncé lors de mon déplacement à la *European Cyber Week* de Rennes, le 16 novembre dernier, la mise en place d'un « bouclier cyber » à destination de 750 PME et ETI centré sur des chaines de valeur prioritaires visées par la directive NIS 2. Ce dispositif entend compléter l'action du Gouvernement à destination du tissu économique en proposant un accompagnement de bout-en-bout des bénéficiaires, via le co-financement public de mesures d'audit et d'évaluation des risques, de définition de plans d'action personnalisés et de mise en œuvre de solutions cyber. Il poursuit notamment l'objectif de permettre aux entreprises en sortie de certifier d'un niveau de sécurité qui facilitera la souscription d'une assurance cyber, sur la base d'un référentiel partagé sur l'évaluation du risque qui sera élaboré sous six mois.

Le bouclier cyber est précisément calibré pour veiller à ce que l'action de l'Etat permette de combler des failles de marché en initiant des dynamiques. En effet, s'il est légitime à intervenir en dernier ressort lorsqu'une carence de l'initiative privée a été identifiée, il ne saurait se substituer aux logiques de marché ni supplanter les chefs d'entreprises dans la définition d'une politique de cybersécurité pour leurs organisations. C'est bien à ces derniers de placer la cybersécurité au rang de priorité stratégique et de prévoir les investissements nécessaires, de manière récurrente et pérenne.

Dans cette perspective, je souhaite vous confier la conduite d'un plan de recommandations visant à identifier les leviers privés à mobiliser pour passer à l'échelle en matière de cybersécurisation de nos TPE, PME et ETI. Pour ce faire, vous vous appuierez sur les acteurs de la cybersécurité rassemblés au sein du Campus Cyber et procéderez selon les axes suivants :

- Vous travaillerez à l'élaboration du référentiel partagé sur l'évaluation du risque cyber d'une entreprise en vous appuyant sur les assureurs et acteurs de la filière présents au Campus, en lien avec les autorités administratives compétentes ;
- Vous identifierez les dispositifs permettant de rendre les systèmes d'information des entreprises plus efficients et plus résilients et formulerez des préconisations visant à favoriser leur adoption au sein du tissu économique ;

- Vous rechercherez, en vous appuyant sur l'image et le positionnement uniques du Campus, les voies et moyens de sensibiliser de nouveaux segments d'entreprises aux enjeux de cybersécurité, au travers de réseaux territoriaux et de leurs interlocuteurs de proximité naturels ;

- Vous mobiliserez les acteurs du Campus afin de contribuer à la structuration d'une offre compétitive et non subventionnée de conseil et d'audit en cybersécurité à destination des entreprises pour massifier l'ambition du bouclier cyber malgré le caractère transitoire du financement public ;

- Vous veillerez à ce que les membres du Campus soient impliqués dans les travaux de la filière des industries de sécurité visant à recenser les services et solutions cyber existants, notamment en vue de constituer un catalogue d'offre souveraine claire et lisible, dynamiquement mise en valeur par types de solutions, et réactualisé chaque année, et qui doit devenir à terme un bien public ;

- Le cas échéant, vous pourrez identifier les ressorts et mécanismes par lesquels cette offre pourrait être davantage promue auprès des bénéficiaires de programmes d'audit de cybersécurité, notamment ceux cofinancés sur fonds publics, qu'il s'agisse de la mise en œuvre du dispositif « bouclier cyber » ou des dispositifs développés par les régions.

Dans ce cadre, vous pourrez faire appel à l'ensemble des structures représentant l'écosystème cyber à vos réflexions, notamment la DGE, l'ANSSI et le GIP ACYMA. Dans la même logique, vous veillerez également à ce que vos réflexions s'inscrivent en complémentarité avec le programme d'accompagnement à la cybersécurisation des TPE-PME que Bpifrance s'apprête à déployer au cours de l'année 2023.

Vous me remettrez un bilan intermédiaire de vos avancées fin février 2023 et vos conclusions définitives à la fin du mois d'avril.

Jean-Noël BARROT

Synthèse des réponses au questionnaire

Des dispositifs publics et privés existent sur toute la chaîne des besoins des TPE/PME, de la sensibilisation à la réponse à incident. Toutefois, leur manque de lisibilité étant élevé, et le marché des TPE/PME étant particulièrement difficile à adresser, le besoin de travailler sur une place de marché accessible, orientant les entreprises selon leur localisation, secteur et maturité, semble s'ériger en priorité.

Dispositifs de sensibilisation :

De **nombreux guides de bonnes pratiques, formations, campagnes de sensibilisation, existent.** Toutefois, ils ne sont **pas toujours accessibles** aux plus petites TPE/ PME. Leur **implantation territoriale** est plutôt bonne, grâce aux relais des associations et de l'ANSSI en région, ainsi que des futurs Campus Cyber territoriaux. Pour **massifier la sensibilisation**, les **acteurs privés** peuvent aussi jouer un rôle en **sensibilisant les fournisseurs, prestataires,** voir en rendant des obligations de sécurité obligatoires.

Dispositifs de prévention (diagnostic et mise en œuvre de solutions) :

Beaucoup de dispositifs existent, souvent spécifiques à une région ou un secteur. A échelle nationale, pour les TPE / PME, BPI et Cybermalveillance.gouv.fr et son réseau d'experts cyber labellisés sont incontournables. Beaucoup d'offres privées existent également, dont les coûts sont variables. Certains industriels proposent à leur fournisseurs un audit de maturité cyber. La méthode des parcours de l'ANSSI (non destinée aux TPE PME) est intéressante à retenir, car va au-delà du simple diagnostic.

On note des **disparités fortes entre les secteurs :** le secteur aérospatial, via le dispositif Boost Aerospace, semble l'un des plus mature. Un référentiel a été défini, et les chaînes d'approvisionnement sont incitées à évaluer leur maturité. Le secteur de la défense est également fortement accompagné, via la DGA[1]. Pour le secteur de l'énergie, le dispositif PME Cyber de la DGE[2] permettra l'accompagnement de 750 PME.

Il est également à noter que de **nombreuses initiatives régionales existent.** Certaines régions prennent ainsi en charge partiellement les investissements cyber des entreprises via notamment des chèques cyber.

Dispositifs de réponse à incident :

Les **12 CSIRT régionaux** progressivement mis en place sont en mesure de répondre aux besoins des entreprises à échelle territoriale. Le réseau de **Cybermalveillance.gouv.fr** est également un dispositif capable de mettre en

[1] Direction Générale de l'Armement
[2] Direction Générale des Entreprises

relation les entreprises avec des prestataires. Enfin, **l'OCLCTIC accompagne les entreprises jusque dans le dépôt de plainte,** processus encore trop peu généralisé car peu évident pour les TPE / PME.

Synthèse des principales difficultés identifiées :

Cette offre **n'est pas lisible** (notamment les nombreux catalogues / labels), elle ne **s'appuie pas sur un référentiel commun de maturité** et d'évaluation cyber, et **manque parfois de transparence**.

De leur côté, les TPE-PME **ne comprennent pas toujours le vocabulaire** ("cyber risque", "résilience", "exposition") ou la différence entre "audit" et "diagnostic", elles n'ont **pas conscience des risques ou minimisent les impacts,** et n'ont pas toujours une transition numérique assez mature. Elles peuvent aussi subir le **manque d'intérêt de leur direction,** à cause de l'image peu pragmatique et opérationnelle des dispositifs de diagnostics et de sensibilisation.

Synthèse des suggestions recueillies :

Pour structurer l'offre, améliorer la pertinence des dispositifs, et passer à l'échelle	S'appuyer sur les **notions de filières,** qui partagent des référentiels et des objectifs communs. S'inspirer par exemple du secteur aérospatial ou de la défense, qui partagent le même référentiel de risques.
	Effectuer une **approche par les impacts** pour que les entreprises comprennent les risques encourus selon leur taille et leur secteur
	Prioriser les sujets de résilience de l'entreprise contre les rançongiciels et les tentatives de vol de données personnelles, plutôt que l'hygiène informatique en général. Commentaire d'une entreprise : *"De notre point de vue, un diagnostic est utile mais n'est pas vraiment la priorité. S'agissant des deux attaques les plus fréquentes, les entreprises sont vulnérables et il est nul besoin d'un audit pour le déterminer."*
	Transposer les parcours adaptés aux différents niveaux de maturité du volet cyber de France Relance aux PME / TPE. Dans la même idée, **segmenter l'offre de services par niveau de maturité en cyber** et niveau de complexité du SI (pas forcément corrélé à la taille d'entreprise).
	Travailler sur des référentiels communs conçus en lien avec les **législations à venir type Cyber Résilience Act**
	Plateforme de scoring du niveau de risque cyber d'une entreprise
	Développer un diagnostic flash ou trousse de secours cyber grand public via un AAP. Il devrait s'appuyer sur des audits

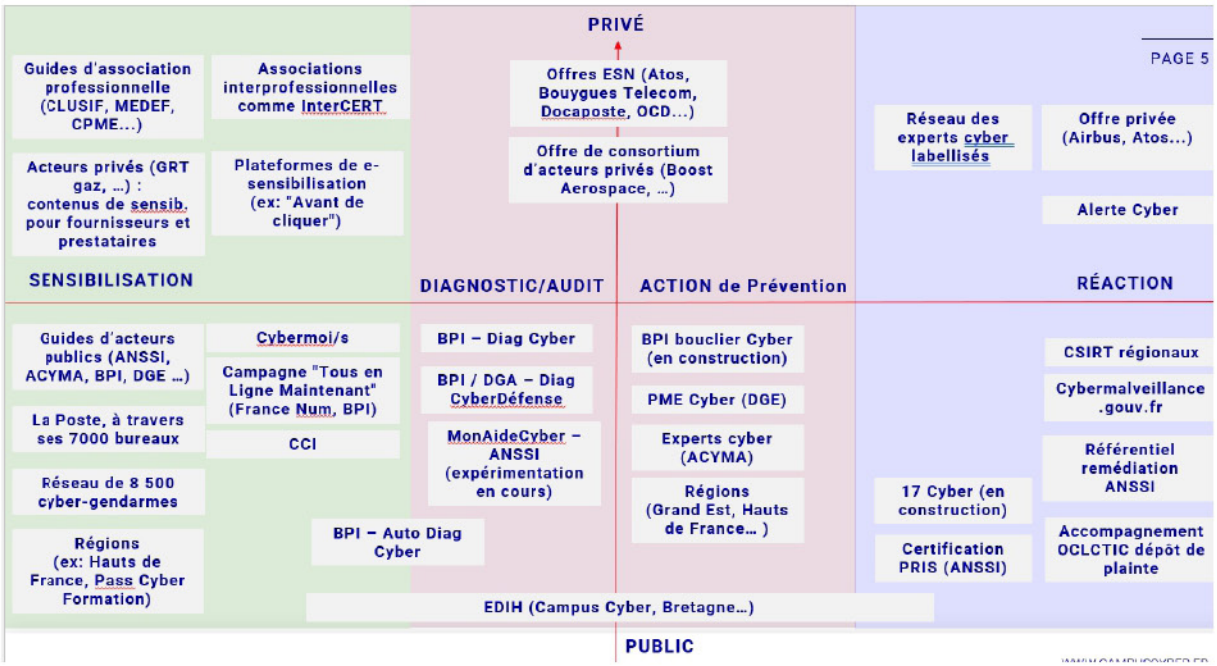
	automatiques en ligne, automatisés et ne nécessitant pas d'approche individualisée au départ.
Pratiques proposées nécessitant réglementations	L'obligation de désigner une personne en charge du sujet
	Analyse de risque systématique et périodique, minimum annuelle
	Exercice de crise annuel
	Formation obligatoire annuelle des dirigeants
	Brevet de secouriste cyber
	Aller progressivement vers une prise en charge obligatoire par les entreprises du risque cyber, à l'instar des mesures obligatoires de protection contre le risque incendie, mesure à mettre en place de concert avec les assureurs.

Synthèse des indications recueillies sur le rôle que devrait jouer le Campus Cyber :

Sensibilisation	Forte attente sur le rôle du Campus dans l'organisation de campagnes de sensibilisation, dans l'organisation de conférences, de formations / sessions d'informations à destination des PME … Il peut pour cela **faire contribuer ses membres**. Le Campus Cyber est pour beaucoup **l'opportunité de créer du lien et une manière d'animer la sensibilisation,** soit en produisant du contenu, soit en mutualisant les contenus existants.
Agrégation, mutualisation, diffusion	Le Campus peut **agréger les offres existantes** (formation, diagnostic, tout dispositifs existants) et **en faire la promotion**. Un **catalogue lisible** des produits et services délivrés, au moins par les acteurs engagés auprès du Campus, est fortement attendu. Le Campus pourrait **promouvoir les solutions émergentes** au niveau des **pouvoirs publics,** y compris au niveau européen. En tant que **vitrine,** le Campus peut aussi **valoriser les success story** françaises et s'en servir comme de démonstrateurs. Le Campus pourrait **relayer les communications sur les menaces,** ainsi que les **priorités à adresser** (annuellement ?) à destination des TPE-PME.
Fédération des acteurs, promotion de la souveraineté	Le Campus est attendu dans la **mise en relation** qu'il peut permettre entre les TPE PME ETI et les ESN françaises. Il pourrait dynamiser les échanges, identifier et **faire émerger les acteurs locaux** via les Campus Cyber territoriaux, organiser des **rencontres utilisateurs/ offreurs**, voir proposer une market place. Les

	partenariats et relations étroites avec les organisations représentatives des PME et TPE, et avec les Régions, est essentiel. Enfin, il peut **favoriser le rayonnement des associations**. A terme, son rôle de **vitrine du savoir-faire français** en cybersécurité à l'international est attendu.
Gouvernance des dispositifs de sécurisation des TPE-PME	En incarnant une posture de **tiers de confiance**, le Campus pourrait soutenir **et être garant des dispositifs mis en place.** Certains évoquent aussi qu'il puisse permettre une bonne utilisation des subventions de l'Etat. Enfin, il pourrait engager des efforts et avoir des effets de leviers en travaillant à l'intégration d'options de sécurité obligatoires dans les packages télécoms vendues aux TPE PME, et en poussant la nécessité d'obligations de sécurisation des progiciels ciblant ces mêmes entreprises.
Campus Cyber Territoriaux	Ils interviennent en **coordination et mise en visibilité des actions locales**, et peuvent **remonter les « besoins terrains »**, grâce à leur connaissance fine de l'écosystème. Les acteurs interrogés rappellent que c'est au niveau territorial que se noue **la relation de confiance** avec les TPE PME. Cet ancrage est donc primordial. Attente également dans l'aide et **le partage des initiatives européennes et nationales de financement** de la cybersécurité.

Cartographie (non exhaustive) des dispositifs



Bpifrance travaille à la mise en place de plusieurs dispositifs à destination des entreprises :

- Déployé depuis mars 2023, le Diag Cybersécurité est un module d'accompagnement de 4 jours hommes, dont l'objectif est de dresser un état des lieux et d'établir un plan de sécurisation des systèmes d'information. 100 PME devraient être accompagnées lors de la première année du dispositif. Son coût est de 4400 €HT, pris en charge à 50% par Bpifrance.
- Bpifrance travaille en étroite collaboration avec la DGE et l'ANSSI pour élaborer un dispositif d'accompagnement à destination des PME-ETI critiques, comportant un diagnostic, un plan de sécurisation et l'appui à la mise en œuvre du plan de sécurisation, notamment via l'acquisition de solutions. Son déploiement est prévu à l'automne 2023
- Le bouclier cyber est une solution de sécurisation managée destinée à outiller les PME. Les solutions ont été sélectionnées avec l'appui du Campus Cyber à la suite d'un appel à manifestation d'intérêt adressé à l'écosystème d'offreurs de solutions français. Les deux lots retenus portent sur une offre de sécurisation managée et sur la sauvegarde. Son déploiement est également prévu à l'automne 2023

PME cyber

La DGE proposera à compter de septembre le dispositif « Cyber PME » dont l'objectif principal est de faire monter en compétences les PME et ETI en matière de cybersécurité. Pour cela, le dispositif repose sur une approche de bout-en-bout qui va du diagnostic à l'implémentation d'un plan d'action, y compris achat de solutions. Ce dispositif est ouvert à tous les secteurs bien qu'il vise à cibler en

priorité les sous-traitants d'acteurs majeurs du secteur de l'énergie et de l'aérospatial.

Alerte Cyber

Un dispositif d'alerte cyber à destination des plus petites et moyennes entreprises existe depuis 2021, s'inspirant des alertes météo.

L'idée est de fournir une notice succincte et compréhensible aux dirigeants d'entreprises lorsqu'une vulnérabilité ou une campagne d'attaque critique est identifiée.

Réalisée par Cybermalveillance.gouv.fr et l'ANSSI, 6 acteurs de proximité des entreprises ont été chargés de relayer ces alertes le plus largement possible : le MEDEF, la CPME, l'U2P, les chambres de commerce et d'industrie, les chambres de métiers et de l'artisanat et FranceNum. Cela représente près d'un million de destinataires.

Réseau labellisé expert cyber de Cybermalveillance.gouv.fr

Cybermalveillance.gouv.fr est la plateforme du groupement d'intérêt public ACYMA dont la mission est la prévention, l'accompagnement et l'assistance aux particuliers, entreprises, associations et administrations victimes d'actes de cybermalveillance.

L'un des services proposés par Cybermalveillance.gouv.fr au titre de sa fonction de "guichet unique" est la mise en relation des publics particuliers comme professionnels avec un réseau de plus de 1250 prestataires de proximité, référencés sur l'ensemble du territoire, dont plus de 200 sont labellisés ExpertCyber, en capacité d'apporter une assistance technique pour répondre aux incidents.

17 cyber : Dispositif national de sensibilisation, prévention et d'assistance aux victimes

Porté par le ministère de l'Intérieur, le projet du 17Cyber a pour objectifs d'apporter une assistance aux victimes et un accompagnement vers la judiciarisation des faits de cybercriminalité. Le dispositif s'appuiera sur la plate-forme Cybermalveillance.gouv.fr où les victimes pourront échanger par tchat avec un policier ou un gendarme une fois l'incident de cybersécurité identifié et les premiers conseils prodigués.

AirCyber par BoostAeroSpace, le programme unique d'entraide et d'évaluation de maturité cyber collaboratif de la filière Aérospatiale et Défense.

AirCyber est la réponse collaborative des donneurs d'ordre européens (Safran, Thales, Dassault et Airbus, …) aux problèmes de maturité des petits acteurs de la chaîne d'approvisionnement. Depuis 2019, ce service de gouvernance cybersécurité a été mis à disposition de plus de 300 entreprises PME/ETI du

secteur, dans le but final d'harmoniser vers le haut le niveau de cyber résilience de toute la filière.

- Aperçu du service / plateforme de gouvernance cybersécurité fournisseurs / équipementier :
  - Evaluation de maturité sur questionnaire et plan d'actions continus (selon niveaux : bronze, silver, gold) validés et adaptés par un expert sur site (choix parmi 10 sociétés);
  - Suivi mensuel en ligne et annuel avec un expert cybersécurité ;
  - Portail de chiffrement de données confidentielles ;
- Aperçu des outils communautaires de montée en maturité :
  - Catalogue collaboratif de solutions (300 services et produits référencés) cyber de confiance (marketplace de mise en relation collaborative de solutions, rating, score de confiance en fonction du déploiement …)
  - Offre d'accompagnement au plan d'action AirCyber (RSSI à temps partagé) via 6 sociétés françaises expertes ;
  - Communauté AirCyber physique et en ligne (webinars mensuels de communauté, conférence annuelle de resensibilisation, partage / création de documents cyber, bonnes pratiques de cybersécurité, retours d'expérience, news régulières, observatoire sécurité …)

European Digital Innovation Hub (EDIH) : exemple de CYBIAH, pour l'Île-De-France

Prévu par la Commission européenne dans le cadre du programme « Digital Europe », les EDIH sont des dispositifs régionaux ayant pour objectif de soutenir et d'accélérer la transformation numérique des acteurs économiques d'un territoire, et notamment les TPE et PME.

En Île-de-France, L'EDIH CYBIAH s'est donné pour objectif de faire monter en maturité digitales 120 PME franciliennes. Le consortium est composé de 12 membres, dispose d'un budget de 6 millions d'euros via des subventions européenne et régionale, et le programme initial durera 3 ans.

Groupe de travail sur l'assurance cyber, Direction générale des Entreprises

Ce groupe de travail piloté par la DG Trésor vise à faciliter la souscription de contrats d'assurance cyber pour les entreprises – notamment TPE/PME/ETI – afin de permettre le développement du marché de l'assurance cyber en France. Une meilleure compréhension des éléments utiles aux assureurs est de mise, et passe dans un premier temps par l'élaboration d'une synthèse des différents référentiels de cybersécurité existants afin d'établir une « grammaire » commune de la cybersécurité des entreprises.

L'objectif du premier livrable du groupe est de rassembler l'ensemble des référentiels de référence existants pour en faire une compilation globale mettant en lumière les principaux points de la cybersécurité d'entreprise, en distinguant entre grandes entreprises et ETI d'un côté et TPE/PME d'un autre. Ce premier livrable devrait être validé dans le courant de l'automne.

Exemple du rôle joué par les acteurs privés : secteur banques et assurances

Depuis de nombreuses années, les acteurs privés s'impliquent dans la cyber sécurisation des PME.

Par exemple, le secteur des banques et assurances joue un rôle dans la sensibilisation des entreprises vis-à-vis de la cybermenace. Les établissements organisent en effet des évènements de sensibilisation, communiquent sur les schémas de fraude visant les entreprises, peuvent proposer l'installation gracieuse de moyens de lutte contre la fraude, et portent les solutions étatiques (cyber malveillance, signalement, etc.) à la connaissance de la clientèle.

Depuis plus récemment, ces organismes construisent des offres de conseil et d'accompagnement pour leurs clients.

Synthèse des questionnaires des services économiques des ambassades (7 pays)

Afin de s'inspirer des modèles mis en place ailleurs, nous avons posé des questions sur les pratiques en place concernant la cybersécurité des PME aux Services économiques[3] des ambassades de la France dans les pays suivants : **l'Allemagne, le Royaume-Uni, l'Estonie, le Danemark, le Canada, les Etats-Unis, et Israël.**

Nous remercions les Services économiques pour leurs réponses. Les informations recueillies permettent de confirmer plusieurs constats, et d'identifier des bonnes pratiques dont la France pourrait s'inspirer.

CONSTATS :

Il semble que pour chacun des services interrogés, la menace cyber pesant sur le tissu économique des PME est identifiée comme majeure. Pour y faire face, de nombreux dispositifs ont été mis en place ces dernières années, et la majorité d'entre eux sont adressés aux grandes entreprises.

Plusieurs répondants indiquent que les PME ont une mauvaise connaissance de ces dispositifs et des interlocuteurs vers lesquels se tourner quand elles font face à une cyberattaque.

Les répondants indiquent ne pas disposer d'un catalogue répertoriant les offres de cybersécurité souveraines.

Certaines réponses confortent les difficultés identifiées en France. Par exemple, l'Estonie mentionne deux difficultés principales rencontrées dans le processus de cyber sécurisation des TPE-PME : d'abord, il est difficile d'atteindre ce public dans la durée, car peu d'entreprises peuvent se permettre d'avoir une personne travaillant spécifiquement sur le sujet de la sécurité numérique. D'autre part, elle observe une tendance à la surestimation des capacités et des connaissances en sécurité numérique chez certains dirigeants de TPE-PME, qui appliquent encore des recommandations obsolètes partagées il y a plusieurs années, qu'il faudrait de fait actualiser.

SYNTHESE ET BONNES PRATIQUES IDENTIFIEES PAR PAYS :

En Allemagne, la cybersécurité est une compétence fédérale depuis 2022, année au cours de laquelle une nouvelle stratégie nationale de cybersécurité a été publiée. La politique de numérisation des TPE-PME y est pensée de pair avec celle de leur cyber sécurisation. Par exemple, le programme d'accompagnement Go-Digital propose un module de sécurité informatique subventionné.

[3] Les Services économiques sont chargés de décrypter la situation économique des pays au sein des Ambassades.

Depuis 2020, le Centre de Transfert pour la sécurité informatique des PME est au cœur du dispositif. Ce centre ne propose pas d'aide directe aux PME, mais il **regroupe toutes les offres de cybersécurité disponibles, et oriente les TPE-PME selon leurs spécificités**. L'équivalent allemand de l'ANSSI, le BSI, est chargé de la protection des Opérateurs d'Importances Vitales.

En 2022, la fédération des chambres de commerce et d'industrie pointe les manquements de l'Etat en matière de cybersécurité, et signale que près d'une entreprise sur trois souhaite davantage de soutien de la part du gouvernement en cas de cyberattaques, car une fois le sinistre survenu, elles ne savent pas à qui s'adresser pour obtenir de l'aide. De même, d'après la fédération, la plupart des entreprises ont pris des mesures techniques, mais au niveau de la sensibilisation des collaborateurs, il y a encore un effort à mener, et une aide pour la mener est demandée par les entreprises.

Au Canada, la cybersécurité des PME est une priorité, le questionnaire soulignant l'importance majeure de ces acteurs dans le tissu économique canadien.

Une difficulté similaire à l'Allemagne est signalée : plus de la moitié des PME victimes de crise cyber ne savent pas à qui s'adresser, et 85% ne savent pas ce que le gouvernement du Canada offre en matière de cybersécurité.

Le Centre canadien pour la cybersécurité, créé en 2018, constitue une **source unifiée de conseils, d'avis, de services et de soutien spécialisés** pour le grand public et les entreprises. Il existe aussi des initiatives provinciales propre. Il existe enfin une **certification "cyber sécuritaire Canada" adressée aux PME**, initiative publique-privée. Par ailleurs, le Canadian Cyber Threat Exchange (CCTX), mis en place en 2015, est une solution privée d'échanges des meilleures pratiques, méthodes de cyber-sécurisation et de partage d'actualité sur les menaces cybers.

Au Danemark, la dernière stratégie nationale de cybersécurité date de 2021. Une diversité de dispositifs existe, dont certains visent spécifiquement les TPE-PME. Un **portail unique** permet aux entreprises danoises de réaliser leurs démarches en cas d'incidents de cybersécurité.

Dans le contexte de l'invasion russe de l'Ukraine, l'ancien ministre de l'Industrie, des Entreprises et des Affaires financières a annoncé la mise en place d'un **fond destiné au renforcement de la cybersécurité des TPE-PME,** ayant également vocation à leur permettre d'obtenir une licence ou une certification.

Il n'existe pas de référentiel sur l'évaluation du risque cyber public, mais des initiatives privées existent comme le "D-seal" : un **programme de labellisation**

privée pour la sécurité et la résilience informatique, et l'utilisation responsable des données.

Les interlocuteurs de proximité des TPE-PME sont rassemblés via le **"pacte de cybersécurité"**, qui vise à coordonner et faciliter les initiatives privées en matière de cybersécurité (y compris les campagnes de sensibilisation et de prévention).

Aux Etats-Unis, le "NIST Small Business Cybersecurity Act" exige que le **NIST** (Instituts des standards et de la technologie) **tienne compte des petites entreprises quand il élabore des directives**. Les Etats ont par ailleurs adopté un "Small Business Cyber Training Act", qui exige que 5 à 10 % du nombre total d'employés des principales Small Business Development Centers (SBDC), aient reçu une formation cybersécurité certifiante pour leur permettre de fournir une aide aux petites entreprises dans ce domaine.

S'agissant des acteurs du secteur privé, les **assureurs et les courtiers en assurance** jouent un rôle croissant dans la sensibilisation et l'accompagnement de leurs clients en matière de cybersécurité.

Enfin, des États fédérés et municipalités montent également des **taskforces, conseils et initiatives dédiés à la cybersécurité,** mêlant des acteurs issus du secteur public, privé ou universitaire, avec pour ambition d'accroître le niveau de préparation en matière de cybersécurité pour les acteurs publics et privés. Par exemple, en 2019, l'Université de l'Indiana, grâce à des financements issus du secteur privé et de l'État de l'Indiana, a mis en place une clinique cyber, proposant des formations à destination du secteur public, des dirigeants d'association ou de petites et moyennes entreprises locales.

En Estonie, les TPE PME représentent + de 99% des entreprises. L'équivalent de l'ANSSI est la RIA. Là aussi le secteur privé est largement exposé aux risques, et malgré le secteur public estonien considéré comme "modèle" en la matière, le questionnaire indique des fortes lacunes dans le secteur privé. La principale source de cybersécurité en Estonie reste l'authentification numérique par le biais des **cartes d'identité numériques.**

Comme en France, le RIA considère que le meilleur moyen d'assurer la résilience face aux cyberattaques reste le **partage d'informations.** Ce partage doit avoir lieu avec les individus (ce qu'ils doivent faire dans les différentes situations d'urgence, partage de bonnes pratiques au quotidien), mais aussi avec les autorités (que ce soit manuellement ou automatiquement), et entre les différents acteurs de l'économie. Il n'existe pas de catalogue, mais l'écosystème est très centralisé et donc connu de tous.

Les principaux interlocuteurs à disposition des entreprises sont le RIA et la police, ainsi que les banques dans une moindre mesure. Les **opérateurs télécoms et fournisseurs d'accès à Internet** peuvent également être sollicités, notamment en cas de pics d'activité cyber malveillante (campagne de phishing importante, nouvelles méthodes qui se répand). Il revient de la part des autorités interrogées la nécessité d'**avoir des informations à jour,** beaucoup d'acteurs disposant d'informations obsolètes, sans formation adaptée aux dernières menaces.

En Israël, l'Israel National Cyber Directorate (INCD), équivalent de l'ANSSI, est le centre du dispositif israélien de coordination de la cyberdéfense du pays. Son objectif est de sécuriser l'ensemble de la société sans distinction, d'autant plus que la notion de PME ne répond pas à la même définition que dans les autres pays interrogés. Toutefois, les critères de cyberdéfense diffèrent selon les secteurs. On constate une priorité commune, qu'est la sécurité numérique des chaînes d'approvisionnement des entreprises stratégiques.

Dirigé par l'INCD, le CERT, centre de commandement d'intelligence opérationnel, dispose d'un **numéro d'urgence accessible aux entreprises et aux citoyens 24 heures sur 24,** afin de répondre aux crises cyber. Il fonctionne grâce à des étudiants spécialisés. Des CERT sectoriels sont en cours de déploiement.

Par ailleurs, l'INCD a créé une **place de marché,** mettant en relation les experts en cybersécurité avec les entreprises. Les entreprises expertes sont soumises à une **"certification légère".** Il n'existe pas de subvention particulière à destination des entreprises, l'Etat estimant que le risque cyber est "un risque comme les autres".

Enfin, le pays estime que la **sécurité intégrée par défaut et par design est plus efficace qu'une sensibilisation à la sécurité cyber a posteriori.** Ils comparent la sécurité cyber à la sécurité routière : "Ni en Europe ni en Israël on ne peut vendre de voiture sans ceinture de sécurité et seulement en recommandant de la poser ! ".

Au Royaume-Uni, 39 % des entreprises déclarent avoir été victimes d'une cyber-attaque en 2022, et 83 % de ces entreprises déclarent avoir subi une attaque par ransomware. La stratégie nationale de cybersécurité a été mise à jour en 2022.

Le National Cyber Security Center (NCSC), créé en 2016, constitue l'équivalent de l'ANSSI. **L'une de ses missions est notamment de sensibiliser des entreprises.** Cette mission s'opère à travers des campagnes de sensibilisation, des guides de bonnes pratiques. Le gouvernement a également entrepris un partenariat avec l'industrie pour favoriser cette sensibilisation.

Le gouvernement développe également des dispositifs destinés aux entreprises tels que les programmes *Cyber Essentials* et *Cyber Essentials Plus*. Ils permettent de **tester les systèmes d'informations d'une entreprise**, et si le test est considéré comme réussi, l'entreprise se voit délivrer une **certification attestant de son niveau**. De même, il existe un *Cyber Assessment Framework*, **cadre d'évaluation plutôt**

adressé aux grandes entreprises, permettant une auto-évaluation de leur niveau de protection à travers 14 principes.

Au niveau régional et local, des dispositifs existent pour aider les entreprises à se protéger face aux cyber-attaques. Au titre des initiatives privées, le *National Cyber Resilience Centre Group* constitue un **partenariat entre la police, le secteur privé et le monde universitaire,** dont l'un des objectifs est le renforcement de la cyber-résilience des PME.

La nouvelle stratégie cyber annonce la volonté du gouvernement de travailler plus étroitement avec le **secteur assurantiel,** en particulier pour permettre un meilleur partage d'informations sur l'impact des cyber-risques. De plus, le gouvernement entend proposer de nouveaux dispositifs permettant de **signaler plus facilement** les cyber-attaques, et de **mieux soutenir les victimes.**

Liste des personnes et entités entendues

Nous remercions les personnes ayant participé aux auditions :

Marc Bothorel, référent national cybersécurité CPME

Lionel Chaine, DSI de BPI

Marie-Pierre de Bailliencourt, directrice générale de l'institut Montaigne

Dorothée Decrop, déléguée générale d'Hexatrust

Jean-Baptiste Demaison, responsable de l'incubateur de l'ANSSI

Maxence Demerle, VP digital economy task force du MEDEF

Maxime Donadille, conseiller technologies d'avenir, espaces immersifs et cybersécurité du ministre délégué chargé du numérique

Georges Etienne Faure, directeur du pôle souveraineté numérique au SGPI

Benoit Fuzeau, Président du Clusif

Franck Gicquel, directeur des partenariats d'ACYMA (cybermalveillance.gouv.fr)

Sandy Sanders, coordinateur sectoriel de l'ANSSI

Delphine Gomes de Sousa, cheffe du bureau Opération & partenariat de l'ANSSI

Matthieu Heslouin, Chief digital officer de BPI

Florent Kirschner, coordinateur de la stratégie nationale cybersécurité

Mylène Larbi, adjointe au chef de bureau Entreprises et intermédiaires d'assurance

Marie-Liane Lekpeli, directrice de projets numérique responsable et sécurité

Eric Malière-Albrecht, commandant de police (OCLCTIC)

Gwenaelle Martinet, cheffe de projet France Relance à l'ANSSI

Jerome Notin, directeur général d'ACYMA (cybermalveillance.gouv.fr)

Paul Pastor, délégué cybersécurité chez Numeum

Guillaume Poupard, directeur général adjoint de Docaposte

Barnabé Watin-Augouard, colonel de gendarmerie du ComCyberGend

Nous remercions toutes les structures ayant répondu au questionnaire :

Acteurs publics

- ANSSI
- BPI
- ACYMA - Cybermalveillance.gouv.fr
- CCI Paris IDF
- Gendarmerie nationale
- Ministère de l'économie et des finances
- Ministère de l'économie et des finances
- Ministère de l'Intérieur

Associations

- ACN
- AFNIC
- Cefcys
- CESIN
- Club 27001
- Clusif
- CPME
- Gitsis
- Hexatrust
- Hub France IA
- Le Park numérique
- MEDEF
- Numeum
- Pôle d'excellence cyber
- System X
- Systematic Paris-Région
- Women4Cyber

Offreurs

- Advens
- Airbus Cybersecurity
- Apave
- ArcelorMittal
- Arkema
- Atos
- Bouygues
- BoostAerospace
- GRTgaz
- HeadMind Partners
- HubOne
- La Poste
- OCD
- OVH
- Safran
- Schneider Electric France
- Stormshield
- Sysdream
- Wavestone

Régions

- Région Bourgogne-Franche-Comté
- Région Bretagne
- Région Grand Est
- Région Hauts-de-France
- Région Nouvelle-Aquitaine
- Région Pays de la Loire
- Région Provence-Alpes-Côte d'Azur

Startup & PME

- Allistic
- Cyber4U
- Cyberjobs
- Dataxium
- Dustmobile
- Epita – Groupe Ionis
- HAAS Avocats
- Hackuity
- HS2
- IMS Networks
- Intrinsec Sécurité
- Logpoint
- Numeryx
- OperaCyber
- Patrowl
- Predimya - Bfore.ai

- Qorum Secur'Num
- Set in stone
- Systemis
- Synetis
- TrustHQ

Nous remercions également les services économiques des ambassades de la France situés en Allemagne, Danemark, Estonie, Israël, Etats-Unis, Royaume-Uni et Canada.

CAMPUS
CYBER