GOUVERNEMENT

Liberté
Égalité
Fraternité

DOSSIER DE PRESSE

18 février 2021

Cybersécurité, faire face à la menace : la stratégie française

Sommaire

Sommaire 3

Éditorial 4

Une menace informatique en forte expansion 7

Etat de la menace cyber 2020-2021 7
Exemples d'actions à l'encontre des cybercriminels 10
Compromission du centre hospitalier de Dax-Côte d'Argent 11

Stratégie nationale pour la cybersécurité 12

La stratégie d'accélération cyber : un programme ambitieux 12
Coopérer et co-construire : la création d'un Campus cyber en 2021 14
Une réponse spécifique pour les territoires 15
Premiers lauréats du « Grand Défi Cyber » 17
Un guide dédié aux TPE/PME et collectivités locales 18

Sensibilisation et hygiène numérique 19

Cybermalveillance.gouv.fr, une plateforme au service du plus grand nombre 19
Identifier les bons relais : le rôle primordial de la Gendarmerie Nationale 20
Les bons réflexes pour protéger la vie numérique des français 21

Éditorial

Bruno Le Maire
Ministre de l'Économie,
des Finances et de la Relance.

À la fois essentielle à la souveraineté des Etats, à la pérennité du développement des entreprises et à la sécurité des citoyens, la cybersécurité est un enjeu majeur du XXI siècle.

La cybersécurité constitue un moteur de croissance important pour les années à venir. Saisissons nous de cette technologie pour nous positionner dans les secteurs économiques de demain : le véhicule autonome, l'internet des objets ou l'informatique en nuage (Cloud) par exemple. C'est maintenant que cela se joue. L'Etat doit viser deux objectifs : garantir la maitrise des technologies critiques en cybersécurité par des acteurs français de confiance et accélérer le développement de ce secteur économique. Pour cela, nous devons renforcer l'offre - notamment en soutenant l'innovation -, et développer la demande, en particulier en renforçant la sécurité de l'Etat et en accompagnant les acteurs privés dans leur démarche de cybersécurisation. Cela ne sera possible qu'en structurant mieux l'écosystème de la cybersécurité et en renforçant l'offre de formation initiale et continue. Ce plan a pour ambition de créer des emplois en France : notre objectif est de doubler les emplois dans la filière d'ici 2025.

Ces préoccupations sont partagées au niveau européen : l'Europe investit dans la cybersécurité et a annoncé en décembre dernier une stratégie européenne sur le sujet qui inclut des mécanismes de coordination et des dispositifs réglementaires visant à mieux nous protéger ensemble.

La stratégie qui vous est présentée aujourd'hui est la traduction concrète de la volonté du Président de la République et du Premier Ministre de soutenir le développement de la cybersécurité en France. Conçue en relation avec les différents acteurs, et financée par France Relance et le Programme d'Investissement d'Avenir, elle s'adresse à tous : particuliers, entreprises et administrations. Je vous invite à vous en saisir dès maintenant.

Cédric O
Secrétaire d'Etat chargé de la Transition numérique et des Communications électroniques.

A la fois moyen de communication, outil de travail et demain pilote de nos véhicules autonomes, le numérique imprègne chaque jour un peu plus notre vie quotidienne. Les outils numériques apportent avant tout un bénéfice à qui sait les maitriser, mais leur développement nous a aussi rendus plus vulnérables face aux attaques cyber. Il est donc du rôle de l'Etat d'accompagner la prise de conscience des utilisateurs du numérique face à ce risque, les aider à s'en prémunir, et soutenir le développement d'une filière française de la cybersécurité.

La stratégie présentée aujourd'hui prévoit ainsi à la fois de renforcer la sécurité numérique de l'État mais aussi d'accompagner les TPE/PME, les citoyens et les territoires pour les aider à mieux se cybersécuriser. Elle a également pour objectif de favoriser la structuration de la filière française de la cybersécurité au travers notamment du Campus cyber.

Cette stratégie se traduit par un effort financier important de la puissance publique et une mobilisation de toutes les administrations. Au total, 1 milliard d'euros dont plus de 700 millions d'euros de fonds publics seront mobilisés dans le cadre de cette stratégie nationale pour la cybersécurité.

Pour développer la cybersécurité au profit de tous, les financements ne suffiront pas. Il est nécessaire de convaincre, de sensibiliser et d'accompagner les utilisateurs au travers d'initiatives telles que cybermalveillance.gouv.fr car la cybersécurité est l'affaire de tous et elle repose sur l'engagement de chacun. Pour être couronnée de succès, cette stratégie cyber devra impliquer tous les acteurs du secteur, et ce dès cette année, comme toutes les actions de France relance. Ensemble et grâce au travail du coordinateur de la stratégie William Lecat nous devons être champion du monde de la cybersécurité. Vous pouvez compter sur mon soutien et sur celui de mes équipes.

Les objectifs clés

➔ **Augmenter le chiffre d'affaires de la filière à 25 Md€ en 2025 (contre 7,3 Md€ en 2019)** et doubler la part des exportations dans ce chiffre d'affaires en passant de 20 % en 2019 à 40 % du CA en 2025.

➔ **Positionner la France par rapport à la concurrence internationale en doublant notamment les emplois de la filière** pour passer à 75 000 en 2025 contre 37 000 aujourd'hui.

➔ **Structurer la filière et repositionner la France par rapport à la concurrence internationale** en nombre d'entreprises.

➔ **Faire émerger trois licornes françaises en cybersécurité** à l'horizon 2025 en s'appuyant sur les grandes startups du secteur et notamment celles membres du French Tech 120.

➔ **Diffuser une véritable culture de la cybersécurité dans les entreprises** et notamment les plus petites d'entre elles afin de leur permettre d'optimiser la sécurité de leurs réseaux.

➔ **Stimuler la recherche française en cyber et l'innovation industrielle** par des liens stratégiques entre la recherche publique et la R&D industrielle pour parvenir à plus de thèses et plus de brevets.

Les partis pris de la stratégie

➔ **Développer des solutions souveraines et innovantes** de cybersécurité, aux côtés d'acteurs privés**,** en soutenant la recherche et l'innovation.

➔ **Renforcer les liens et synergies entre les acteurs de la filière** et mobiliser toutes les expertises pour fédérer l'écosystème de la cybersécurité en France par exemple par la mise en place d'un lieu « totem », le Campus cyber (vaisseau mère en région parisienne et déclinaisons dans les régions), sur lequel tous les acteurs du secteur pourront se regrouper dans une optique de mise en cohérence globale et de travaux communs.

➔**Soutenir la demande** (citoyens, entreprises, collectivités et Etat) notamment en renforçant la prise de conscience de la population au risque cyber via des actions de sensibilisation et de mise en valeur de l'offre française.

➔**Former les jeunes et les professionnels aux métiers de la cybersécurité** en adaptant les formations déjà existantes, en en créant de nouvelles et en promouvant cette filière extrêmement porteuse mais encore mal connue du grand public.

Synthèse des montants de la stratégie nationale cyber (nouveaux crédits hors militaires et formation)

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*	720
Part privée	225	74	20	*n.a.*	>319
Financement	**515**	**148**	**176**	**200**	**>1 039**

**Montants prévisionnels*

Une menace informatique en forte expansion

Etat de la menace cyber 2020-2021

En forte augmentation depuis le milieu des années 2010, la menace cyber exploite avec efficacité certaines vulnérabilités inhérentes à la transformation numérique de la société et de l'économie : une forte dépendance des entreprises et des services publics envers leurs services numériques, une prise de conscience encore insuffisante des enjeux de cybersécurité et une facilité croissante d'accès aux outils malveillants.

Les opérations récentes ont souligné une professionnalisation des attaques informatiques, tant dans la phase de reconnaissance préalable des futures victimes que dans celle de l'exploitation à fins de rançonnage ou d'espionnage. De fait, les attaques dirigées contre les entités françaises se caractérisent par une sophistication et une furtivité croissantes.

L'activité opérationnelle récente permet de confirmer les **trois tendances** suivantes.

- La cybercriminalité constitue la principale menace cyber pour les entreprises, les collectivités locales et certains organismes publics tels que les établissements de santé, au travers d'une multiplication très alarmante des attaques par rançongiciels. Ainsi, à périmètre constant, le nombre de cyberattaques par rançongiciels traitées par l'ANSSI a pratiquement été multiplié par 4 entre 2019 et 2020, passant de 54 à 192.
- Les cybercriminels se professionnalisent et se structurent, mettant au point des modèles d'affaires de plus en plus lucratifs. Outre le chiffrement des données et la paralysie des réseaux, les attaquants multiplient les techniques de chantage pour accroître la pression pesant sur leurs victimes et les pousser à accepter le paiement d'une rançon (publication de données sensibles, revente d'accès à d'autres cybercriminels, *etc.*). Cet écosystème cybercriminel se limite probablement à plusieurs centaines de personnes dont seulement quelques dizaines disposant véritablement de capacités à développer des outils d'attaques performants. L'ANSSI estime que près de la moitié de ces attaques sont le fait de seulement 5 groupes distincts. Néanmoins, les profits colossaux qu'ils réalisent leur permettent d'étendre leurs réseaux et d'être particulièrement attractifs. Difficilement identifiables, souvent hors de portée des mécanismes d'entraide pénale internationale, voire dans certains cas, protégés par des Etats, ces cybercriminels bénéficient souvent d'une impunité. Au-delà du renforcement du niveau de cybersécurité de leurs potentielles victimes françaises, il est encore difficile d'entraver efficacement l'action de ces groupes.
- **Les organismes publics et les collectivités territoriales sont particulièrement vulnérables à ce type de menace**, et ce bien qu'elles ne soient pas en mesure de payer les rançons, à la fois du fait de l'absence de moyens financiers à hauteur des montants réclamés et de la transparence de la dépense publique. Aussi, en 2020, 20 % des victimes de rançongiciels portées à la connaissance de l'ANSSI étaient des collectivités locales, qui ont ainsi connu une mise en péril de leurs activités essentielles de service

public, au plus proche du citoyen. Les établissements de santé, publics comme privés représentent quant à eux 11% des victimes accompagnées par l'ANSSI en 2020, le nombre d'incidents de compromissions par rançongiciels passant de 17 cas en 2019 à 27 cas en 2020. L'ANSSI recense actuellement environ une tentative d'attaque par semaine sur des infrastructures de la chaîne hospitalière.

Le tissu économique de la Nation est également affecté par cette menace qui cible les PME – sans toutefois que l'on puisse estimer précisément leur volume, certaines préférant taire ces attaques et payer les rançons, d'autres n'ayant pas connaissance des dispositifs d'accompagnement et de signalement existants – jusqu'aux groupes multinationaux du CAC40, plus à même d'envisager le paiement de rançons élevées, pouvant s'établir à plusieurs millions de dollars, en échange de la récupération de leurs données.

Graphique : Secteurs d'activité touchés par les rançongiciels en 2020 en France

- **Le risque d'espionnage demeure élevé pour les entreprises stratégiques disposant de savoir-faire industriels rares et évoluant dans des secteurs sujets à une forte compétition internationale**. Au cours des dernières années, plusieurs acteurs sensibles, publics et privés, dont des opérateurs d'importance vitale, ont été victimes de ce type d'attaque, dont l'origine étatique est fortement présumée.
- **L'espionnage par des moyens cyber est également un risque majeur pour les administrations.** Il en est ainsi de la cyberattaque de SolarWinds révélée en décembre, au travers de laquelle un attaquant a pu espionner les administrations américaines les plus sensibles dont les départements de l'énergie, de la défense et du Trésor.
- **Certains attaquants semblent s'attacher à préparer les conflits de demain.** Cette tendance particulièrement préoccupante consiste à prendre pour cible des infrastructures critiques au travers d'actions de cartographie de réseaux et de prépositionnement d'implants informatiques, dont les objectifs restent difficilement identifiables. Il pourrait s'agir soit d'opérations de reconnaissance en vue de préparer des actions de sabotage avec un impact significatif sur la sécurité nationale, soit d'actes d'intimidation visant à influencer immédiatement la posture des États ciblés dans un contexte de tensions géopolitiques.

Attaques récentes

2019

Juin

Une cyberattaque basée sur une demande de rançon a fait chuter de 35% le bénéfice semestriel du **Groupe Eurofins.**

Oct.

Le **Groupe M6** a été la cible d'une attaque informatique malveillante.

La dernière cyberattaque d'ampleur signalée par un média en France était celle de TV5 Monde en 2015.

Nov.

Le **CHU de Rouen** a été forcé de tourner sans ordinateurs après une attaque cyber massive. Les observations médicales ont dû se faire sur papier. L'activité a été extrêmement ralentie.

2020

Janv.

Une attaque par ransomware a touché le siège du **Bouygues Construction**. Les 3 200 employés du siège ont reçu un SMS annonçant une alerte virale et une coupure du *DataCenter Challenger*.

Mars

Suite à une attaque par déni de services (DDos), en pleine crise sanitaire et pendant une heure, l'**AP-HP** a dû couper l'accès aux mails et aux outils à distance pour ses salariés en télétravail.

La Mairie de Marseille et sa métropole ont déploré une attaque est inédite par son ampleur. Les serveurs ont été cryptés à hauteur de 90% contre une demande de rançon.

Avr.

Suite à une cyberattaque, impossible de se connecter aux sites Internet de **la collectivité Toulouse Métropole.** Une panne jugée « extrêmement grave » selon Jean-Luc Moudenc (LR), le maire de Toulouse.

L'entreprise Visserie Service (PME) a été victime d'une cyberattaque destinée à créer de la cryptomonnaie par le biais du serveur informatique de la société après avoir enregistrée des activités suspectes sur son serveur informatique.

Juin

Sans conséquence directe sur la diffusion, **l'activité de France 3** a dû être transférée au siège du groupe audiovisuel suite à une attaque cyber.

Juil.

Les centres de données informatiques de Tourcoing et d'Anzin de **Rabot Dutilleul (Groupe BTP nordiste)** ont été infectés par un virus Netwalker. Les hackers ont réclamés une rançon de 973 bitcoins, soit près de huit millions d'euros.

Oct.

Sopra Steria, entreprise française de services du numérique, a détectée une cyberattaque, intervenue sur son réseau informatique.

Nov.

La société qui gère les importations de carburants et textiles pour le **groupe E.Leclerc, Siplec,** a été victime d'une attaque par ransomware.

Le Groupe **Ouest-France** a été victime d'une attaque de son système informatique, l'obligeant à diminuer son nombre d'éditions pour une journée.

Déc.

Le **Groupe Fareva**, leader mondial de la sous-traitance industrielle, a été la cible d'une attaque par ransomware qui a paralysé son appareil de production. Le préjudice a été estimé entre 25 à 30 millions d'euros.

Pour contrer une attaque cyber, le **Groupe Atlantic**, spécialisé dans les produits de chauffage, a dû ralentir ou cesser ses activités dans certaines entreprises.

Au Centre hospitalier d'Albertville-Moûtiers, une attaque cyber a paralysé un certain nombre d'équipements, de serveurs, de logiciels, et une partie du réseau informatique. Elle a aussi impacté les systèmes de deux **Ehpad** et **Unités de soins de longues** durées du CHAM.

2021

Janv.

Pour **CDER, un cabinet comptable pour le compte du secteur agricole et viticole champenois,** ce sont plusieurs millions d'euros qui ont été dérobées à la suite d'une attaque cyber

Une cyberattaque a paralysé les services des bibliothèques municipales et l'ensemble des sites de la mairie d'**Angers**. Le conservatoire ne pouvait ni recevoir, ni envoyer des mails

Fév.

Le centre hospitalier de Dax (Landes) a fait l'objet d'une cyberattaque. Les services ont été impactés.

L'hôpital de Villefranche-sur-Saône a subi une attaque par un crypto-virus.

Exemples d'actions à l'encontre des cybercriminels

La France conduit des actions au niveau national et international visant à démanteler les réseaux de cybercriminels responsables d'attaques sur son territoire.

La police française aidée de ses homologues ukrainiens a ainsi annoncé mardi 9 février 2021 avoir **arrêté plusieurs personnes agissant pour le groupe cybercriminel Egregor.** Ce groupe, apparu en 2020, **revendique plus de 150 victimes**, dont plusieurs françaises (notamment Ouest France, Ubisoft et Gefco).

Un travail d'investigation, mené conjointement avec Europol, a par la suite permis à la France de remonter la piste des rançons payées en bitcoin par les victimes, permettant de localiser plusieurs suspects en Ukraine et de les arrêter.

Cette opération n'est pas la première intervention conjointement menée par la France pour démanteler un réseau cybercriminel. En janvier 2021, une coalition (France, États-Unis, Pays-Bas, Royaume Uni, Lituanie, Canada, Ukraine) coordonnée par Europol a permis de **démanteler les infrastructures diffusant, via des courriels infectés, le cheval de Troie Emotet.**

Les différentes versions d'Emotet ont infecté près d'1,6 millions d'ordinateurs dans le monde depuis 2014.

Deux ans ont été nécessaires à la coalition pour comprendre et cartographier l'infrastructure utilisée par Emotet, constituée de plusieurs centaines de serveurs situés à travers le monde, puis coordonner des actions permettant de saisir le matériel informatique utilisé pour diffuser le cheval de Troie.

« Quand le diagnostic tombe et confirme l'attaque, la tension est très forte et nos premières décisions sont 100 % opérationnelles. Nos équipes d'astreinte ont d'abord coupé le lien entre l'attaquant et notre réseau par des mesures de fermeture des cloisons et d'isolement. Dans ces moments-là (quand survient une attaque), on réalise à quel point un tel événement traumatise et rapproche à la fois les hommes…

De nouveaux canaux de communication interne ont été mis en place pour prévenir les collaborateurs et maintenir le contact au cours des prochains jours. Cela allait de la messagerie instantanée au papier-crayon et aux déplacements de bureaux en bureaux. »

Jérôme Lefébure, CFO Groupe M6

Compromission du centre hospitalier de Dax-Côte d'Argent

Le 9 février 2021, le centre hospitalier de Dax-Côte d'Argent a signalé la compromission de son système d'information par le rançongiciel RYUK. L'attaque ainsi que les premières mesures prises pour la contenir ont obligé les équipes du centre hospitalier à adopter un mode de fonctionnement dégradé.

Dès la détection du déploiement du rançongiciel RYUK sur une partie du parc informatique du centre hospitalier, les premières mesures d'endiguement ont été mises en place. Celles-ci ont notamment consisté à compartimenter le parc informatique de l'établissement pour freiner la propagation du rançongiciel et à débrancher les connexions à Internet afin de couper l'accès de l'attaquant au réseau et empêcher toute diffusion du rançongiciel vers d'autres entités. Une autre priorité des équipes informatiques de l'hôpital a été de s'assurer de l'intégrité et de la disponibilité des dernières sauvegardes informatiques réalisées.

Depuis le 12 février, une équipe de l'ANSSI est projetée sur site pour accompagner le CH dans ses actions de remédiation et coordonner les prestataires.

Afin de permettre aux équipes du centre hospitalier de disposer à nouveau d'un réseau digne de confiance le plus rapidement possible, et retrouver ainsi un mode nominal de fonctionnement, une équipe de l'ANSSI procède sur place au remplacement du noyau central de l'infrastructure réseau. Ce noyau central, techniquement désigné par « annuaire *Active Directory* », gère de façon centralisée l'ensemble des permissions d'accès au sein du réseau – ceux des utilisateurs, des machines et des applications – et constitue également un outil d'administration et de gestion centrale du réseau. Élément particulièrement critique, susceptible de donner à un attaquant une prise de contrôle complète du système d'information et des données qu'il contient, il doit être assaini en priorité afin de pouvoir restaurer ensuite progressivement l'intégrité du réseau.

Compte tenu de la complexité de l'annuaire *Active Directory*, son remplacement constitue une opération délicate et nécessite une préparation minutieuse. Elle permet d'expulser l'attaquant de la partie la plus critique du réseau informatique compromis.

Hôpital Villefranche-sur-Saône

Les sites de Villefranche-sur-Saône, Tarare et Trévoux de l'Hôpital Nord-Ouest, ont été victimes d'une attaque par le crypto-virus RYUK, un logiciel malveillant qui bloque les données d'un système informatique, et qui ne sont plus accessibles qu'après paiement d'une rançon.

Actions : Afin de limiter la propagation du virus, les postes de travail du centre hospitalier ont été déconnectés à l'exception du standard des urgences. L'ensemble de la téléphonie a été rendue inaccessible. Toutes les équipes hospitalières ont immédiatement mis en place des procédures dites "dégradées"(usage du papier et stylo) pour maintenir cependant la prise en charge des patients. En coordination avec l'Agence régionale de santé Auvergne-Rhône-Alpes, le SAMU et les pompiers, les patients nécessitant le recours aux services d'urgences des sites de Villefranche et Tarare sont orientés vers d'autres hôpitaux ou cliniques. Une cellule de crise a été installée pour organiser le fonctionnement des trois hôpitaux.

Stratégie nationale pour la cybersécurité

La stratégie d'accélération cyber : un programme ambitieux

Cette stratégie **mobilise 1Md€ dont 720M€ de financements publics**. Son volet économique repose sur 5 axes :

- Développer des solutions souveraines de cybersécurité ;
- Renforcer les liens et synergies entre les acteurs de la filière ;
- Soutenir l'adoption de solutions cyber par les individus, les entreprises, les collectivités et l'Etat, notamment via des actions de sensibilisation tout en faisant la promotion des offres nationales ;
- Former plus de jeunes et professionnels aux métiers de la cybersécurité, fortement en déséquilibre ;
- Soutien en fonds propres.

William Lecat, nommé coordinateur national de cette stratégie d'accélération, a pour mission de superviser l'ensemble des actions qui la constitue et est le garant de sa bonne exécution.

Les travaux du pacte productif ont identifié la cybersécurité comme un marché prioritaire, à accélérer afin d'en exploiter tout le potentiel économique et garantir notre souveraineté numérique. Les solutions proposées s'inscrivent en cohérence avec les stratégies en cours et notamment les actions du **Comité stratégique de filière (CSF) « Industries de sécurité »**, dont le contrat a été signé le 29 janvier 2020, et son projet structurant « cybersécurité et sécurité de l'IoT » mais également **la mission de préfiguration d'un Campus cyber** confiée à Michel Van Den Berghe, **le Grand défi cyber** dans le cadre du Conseil de l'Innovation et **l'action « technologies clés »** conduite en inter-administration dans le cadre de la revue stratégique de cyberdéfense, qui consiste à identifier les briques technologiques critiques en cybersécurité et proposer des plans d'action pour assurer la souveraineté numérique de la France.

Plusieurs objectifs sont fixés à l'horizon 2025 :

X3
Chiffre d'affaire de la filière passant de 7,3 Mds€ à 25 Mds€

X2
Nombre d'emploi dans la filière passant de 37 000 à 75 000

+20%
Nombre de brevets enregistrés par le réseau des SATT et France Brevets

X2
Nombre de thèse CIFRE sur 5 ans passant de 15 à 30 thèses

3
Licornes françaises à faire émerger

+30%
Recherche partenariale

Développer des solutions souveraines et innovantes de cybersécurité – 515M€ dont 290M€ de financements publics

Il s'agit de **soutenir la recherche et l'innovation pour assurer une maîtrise sur les technologies d'avenir en cybersécurité**. Cette action se fera dans le prolongement du Grand défi « automatisation de la cybersécurité » et en cohérence avec l'action « technologies clés » de la revue stratégique de cyberdéfense. L'Etat co-financera, au côté d'acteurs privés garants des perspectives commerciales, le **développement de solutions souveraines, innovantes et performantes identifiées comme clés pour notre autonomie stratégique.** Cela assurera ainsi leur compétitivité et la souveraineté numérique de la France, pour un budget total de **400 millions d'euros, dont 200 millions de l'Etat**. En outre, l'Etat co-investira dans l'écosystème, avec l'industrie, notamment à travers la **création d'un incubateur de startups de cybersécurité,** pour un budget total de 50 millions d'euros, ou encore les structures de transfert de technologie. L'accent sera également placé sur la structuration et la stimulation du domaine de la recherche publique. L'Etat a ainsi mandaté le CEA, le CNRS et INRIA pour piloter, pour le compte de la communauté de recherche française, un programme de recherche doté de 65 M€. L'objectif sera de maîtriser l'ensemble des technologies clés nécessaires pour offrir à notre pays une couverture complète et souveraine pour prévenir les menaces.

Renforcer les liens et synergies entre les acteurs de la filière – 148M€ dont 74M€ de financements publics

Cet axe vise à mieux **fédérer l'écosystème de la cybersécurité en France, par la mise en place d'un lieu « totem », le Campus cyber.** Cette mesure se traduira concrètement par l'installation d'au moins 800 personnes issues du secteur (acteurs publics, industriels, et acteurs de la recherche et de l'innovation publique et privée) dans un espace commun d'environ 20 000 mètres carrés en région parisienne, participant ainsi à resserrer les liens entre petits et grands acteurs, et entre industriels et recherche. Cette logique sera déclinée sur des antennes régionales, en veillant à associer efficacement les acteurs académiques. Ce rapprochement doit favoriser l'émergence de solution globales, aptes à concurrencer les offres étrangères sur le même segment de marché, ainsi que des projets communs le partage de données (48 millions d'euros).

Soutenir l'adoption de solutions cyber (individus, entreprises, collectivités et Etat) – 176M€ dont 156M€ de financements publics

L'objectif est de **renforcer la prise de conscience de la population au risque cyber, à travers des actions de sensibilisation**, de stimuler la demande et de mettre en valeur l'offre française dans le même temps, notamment en faisant du Forum International de la Cybersécurité un évènement de référence au niveau mondial. En parallèle, la sécurité numérique de l'Etat doit être renforcée, à travers des projets de mise à niveau portés par l'ANSSI pour un budget de **136 millions d'euros** sur 2021-2022. Les territoires sont tout aussi concernés, un projet industriel global de démonstrateur doit adresser leurs besoins en ce sens, pour un budget initial de 40 millions d'euros. Ce lieu accueillera également des formations de l'enseignement supérieur permettant ainsi des passerelles vers les entreprises.

Former plus de jeunes et professionnels aux métiers de la cybersécurité

La filière de la cybersécurité française fait face à un déficit de main d'œuvre. Pourtant, elle peut être un débouché pour tous les niveaux, de baccalauréat professionnel à doctorant, ainsi que pour différents domaines de formations (techniques et commerciales). La stratégie propose d'établir un meilleur diagnostic des métiers et formations existantes ainsi que d'**adapter les formations à tous les niveaux pour répondre aux besoins**. La formation par la recherche en cybersécurité sera renforcée : développement de l'offre de masters spécialisées et de mention pour des masters dans d'autres filières, augmentation du nombre de doctorants dont thèses CIFRE, formation courte notamment celles proposées par le CNRS à destination des professionnels.

Soutien en fonds propres à nos acteurs – 200M€ de financements publics

Les start-ups jouent un rôle central dans la construction de l'offre de cybersécurité française. Au travers des outils de financement du PIA, **environ 200M€ devraient financer l'écosystème français dans les 5 années à venir**. Ces fonds viendront prolonger l'action d'investissement des fonds FrenchTech Souveraineté, ambition amorçage angels, ambitions numériques ou encore FrenchTech Seed de Bpifrance.

Coopérer et co-construire : la création d'un Campus cyber en 2021

Budget total : 148 M€, dont 74 M€ de financement public

Fédérer l'écosystème de la cybersécurité en France constitue une priorité pour pouvoir rivaliser avec la concurrence internationale La filière française de la cybersécurité doit se structurer, notamment en disposant d'un lieu totem où les professionnels pourraient collaborer au développement de solutions innovantes. A cette fin, l'Etat soutient la création d'un Campus cyber, qui favorisera les collaborations entre acteurs de l'écosystème (grands groupes, startups, PME, organismes de recherche, Etat…), celui-ci étant encore trop fragmenté aujourd'hui.

Localisé dans la tour ERIA à la Défense, le Campus cyber sera prêt à accueillir dans ses 25 900m^2 plus de 1000 experts d'ici la fin du 2ème semestre 2021. Le Campus cyber est fondé sur quatre piliers :

- les opérations : favoriser le partage de données pour renforcer la capacité de chacun à maitriser le risque numérique (détection, capacités de veille, réponse aux incidents, mise en commun de la connaissance sur la menace) ;
- la formation : soutenir la formation initiale et continue des différents publics (agents de l'État, salarié(e)s, étudiant (e)s, personnel en reconversion…) afin de favoriser une montée en compétence globale de l'écosystème (programmes communs, partage de ressources) ;
- l'innovation : développer les synergies entre les acteurs publics et privés (industriels, start-up et centres de recherche) pour orienter l'innovation technologique et renforcer son intégration dans le tissu économique ;

- l'animation : proposer un lieu ouvert, vivant dédié à la programmation d'événements innovants, propice aux échanges et à la découverte des évolutions (conférence, webinaires, showroom, jobdating, etc.)

À ce jour, plus de 60 acteurs, issus d'une pluralité de secteurs, ont indiqué leur volonté de participer au Campus. Parmi ces derniers, certaines administrations (Police judiciaire, Gendarmerie, ANSSI, Cybermalveillance.gouv.fr, etc.) souhaitent disposer d'équipes présentes sur le Campus.

La constitution de la SAS fin décembre et l'adhésion formelle des premiers actionnaires marquent une nouvelle étape de ce projet ambitieux. Des initiatives similaires verront progressivement le jour dans les territoires, constituant un véritable réseau de Campus cyber.

Une réponse spécifique pour les territoires

Dans le cadre de France Relance, le gouvernement alloue **136 millions d'euros sur la période 2021-2022 à un « volet cybersécurité », piloté par l'ANSSI** et destiné à la cybersécurisation de nos territoires**.** Plus largement, ce plan de relance est également une formidable occasion d'intensifier la lutte contre les menaces cyber et les attaques informatiques.

Construit en concertation avec l'ensemble des acteurs concernés (associations d'élus des communes et de leurs groupements, opérateurs de services numériques, cybermalveillance.gouv.fr, gendarmerie nationale…), le volet cyber du plan de relance concerne l'ensemble des collectivités territoriales, quelle que soit leur taille, et tous les organismes publics, en particulier ceux offrant des services directement au profit des citoyens : hôpitaux et organismes sociaux en priorité.

L'importance des moyens alloués à ce volet permet à l'ANSSI de poursuivre une triple ambition :

- élever substantiellement le niveau de sécurité numérique de l'État et des services publics ;
- contribuer au renforcement du tissu industriel français de cybersécurité ;

- créer un effet de levier conduisant à un investissement durable dans la cybersécurité.

60M€ seraient ainsi consacrés aux collectivités territoriales et 25 M€ dédiés aux établissements de santé, permettant ainsi la mise en place d'un accompagnement adapté à chaque bénéficiaire en fonction de leurs enjeux, des impacts potentiels d'une attaque sur leurs réseaux et des moyens disponibles.

« Le 15 novembre 2019, à la veille du week-end, un interne de services d'urgence signale un problème de droits d'accès à une application métier. Peu après, la DSI constate le chiffrement d'une grande partie des postes de travail et serveurs du CHU. Très vite, le diagnostic tombe : c'est un rançongiciel. »

Cédric Hamelin
Responsable adjoint à la sécurité du système d'information, CHU de Rouen

Des « packs de cybersécurité », dont vont notamment bénéficier les établissements de santé, sont proposés par les experts du domaine et les prestataires de service déjà présents sur tout le territoire afin de comprendre le niveau de sécurité cyber de chacun et d'identifier les actions à mener. Les actions de sécurisation les plus urgentes sont ainsi co-financées afin de donner l'impulsion nécessaire à chacun pour mettre en place les moyens adaptés pour assurer sa sécurité cyber sur le long terme.

Par ailleurs, pour développer une protection autonome et efficace sur le long terme des entités publiques, un programme d'incubation à la création de centres régionaux de réponse d'urgence aux incidents cyber (CSIRT) est développé par l'ANSSI, en partenariat avec les régions.

Premiers lauréats du « Grand Défi Cyber »

Lancé en décembre 2019, le Grand Défi cyber a labellisé 11 entreprises qui ont reçu un montant d'aide total de 8,6 M€ (voir carte ci-dessous). Ce soutien aux entreprises du secteur de la cybersécurité arrive en complément d'un accompagnement de l'Etat préexistant dans le secteur à travers des aides à des entreprises comme Cybelangel, lauréate du Concours Mondial d'Innovation et membre du Next40, GitGuardian et Seald (investissement du fonds ambition amorçage angels), Wallix (fonds ambitions numériques) ou encore CryptoNext (FrenchTech Seed).

Les 11 lauréats du « Grand Défi Cyber »

Un guide dédié aux TPE/PME et collectivités locales

Un nouveau guide réalisé par l'Agence nationale de la sécurité des systèmes d'information avec la direction générale des entreprises et le soutien de Cybermalveillance.gouv.fr s'adresse spécifiquement aux petites et moyennes entreprises (TPE, PME). Proposant des fiches courtes et très opérationnelles, ce guide vise à apporter des conseils et solutions concrètes pour accompagner ces acteurs dans la sécurisation de leur activité, et ce en prenant en compte les ressources limitées à dédier à la sécurité informatique. En effet, une partie des risques cyber peuvent être appréhendés et évités grâce à la mise en place de mesures facilement accessibles à ces acteurs économiques.

Sensibilisation et hygiène numérique

Cybermalveillance.gouv.fr, une plateforme au service du plus grand nombre

Cybermalveillance.gouv.fr est le dispositif gouvernemental d'assistance aux victimes d'actes de cybermalveillance, de sensibilisation aux risques numériques et d'observation de la menace sur le territoire français. Ses publics sont les particuliers, les entreprises (hors OIV et OSE), les associations, les administrations et les collectivités territoriales.

Le dispositif est piloté par une instance de coordination, le Groupement d'intérêt public (GIP) ACYMA, composé de près de 50 membres issus du secteur public, du privé et du domaine associatif et qui contribuent chacun à sa mission d'intérêt général.

Sur le volet prévention, la plateforme www.cybermalveillance.gouv.fr :

- met à disposition gratuitement un kit de sensibilisation sur les menaces et les bonnes pratiques à adopter. Ce kit est accessible à tous et traite de sujets tels que les mots de passe, les sauvegardes, les réseaux sociaux, l'hameçonnage, les rançongiciels…
- référence sur une page dédiée l'ensemble de ses ressources et contenus de sensibilisation (vidéos, mémos, fiches réflexes et pratiques, articles…),
- publie régulièrement des articles d'actualité (télétravail…) et des alertes sur ses réseaux sociaux dès qu'une nouvelle malveillance est identifiée.

Le dispositif propose également un programme de sensibilisation aux risques numériques dédié des collectivités territoriales et des élus. Ce programme met à disposition des élus des conseils et ressources (témoignages, conseils, réflexes essentiels pour leur sécurité numérique) pour anticiper les risques et se sécuriser en amont.

Sur le volet assistance : Cybermalveillance.gouv.fr référence sur sa plateforme plus de 1000 professionnels en sécurité numérique répartis sur tout le territoire français en capacité d'aider ses différents publics lorsqu'ils sont victimes. Il recense également sur son site la liste des 45 cybermalveillances traitées dans son outil de diagnostic en ligne.

Acteurs clés de l'innovation numérique et du service public, les collectivités et les entreprises, (particulièrement les plus petits acteurs) doivent pouvoir bénéficier de services et de produits adaptés afin de se protéger efficacement et de se concentrer sur leur cœur de mission au profit de la croissance économique et du citoyen.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Le label ExpertCyber

Le label ExpertCyber est destiné à valoriser les professionnels en sécurité numérique ayant démontré un niveau d'expertise technique et de transparence dans les domaines de l'assistance et de l'accompagnement de leurs clients. Il a été développé par Cybermalveillance.gouv.fr, en partenariat avec les principaux syndicats professionnels du secteur (Fédération EBEN, Cinov Numérique, Syntec Numérique), la Fédération Française de l'Assurance et le soutien de l'AFNOR.

Justifiant d'une expertise en sécurité numérique assurant des prestations d'installation, de maintenance et d'assistance, les professionnels labellisés ExpertCyber accompagnent les entreprises, associations et collectivités depuis la sécurisation de leur système d'information jusqu'à la résolution des cyberattaques.

Pour en savoir plus :
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/label-expertcyber

Identifier les bons relais : le rôle primordial de la Gendarmerie Nationale

La gendarmerie nationale développe dans l'ensemble de son réseau territorial des compétences au plus près des victimes potentielles de cybermalveillances.

Le réseau CyberGEND de la gendarmerie s'appuie d'abord sur des services spécialisés au niveau central : coordination par le Pôle national de lutte contre les cybermenaces, expertise technique avancée au sein du département informatique-électronique de l'IRCGN et enquêtes complexes et internationales du Centre de lutte contre les criminalités numériques (C3N).

Puis, il se décline dans les régions par 11 Antennes du C3N. Rattachées à des sections de recherche à compétence zonale et en lien permanent avec le C3N, elles apportent une réponse judiciaire de haut niveau en proximité des entreprises et collectivités locales. Elles sont par exemple mobilisées, avec l'appui du C3N, dans tous les dossiers de rançongiciels confiés à la gendarmerie nationale.

Enfin, au niveau départemental, les sections opérationnelles de lutte contre les cybermenaces (SOLC), sont l'acteur de proximité de la gendarmerie en matière de cybersécurité. Ainsi, non seulement ces SOLC appuient les enquêteurs locaux dans le champ de l'analyse de supports de preuve informatique ou la prise en compte des victimes, mais elles viennent fédérer les actions de prévention menées dans chacun de ces territoires. Les SOLC viennent appuyer l'action des référents sûreté de la gendarmerie qui rencontrent entreprises et collectivités locales pour assurer le suivi de leur sécurisation physique (et donc leurs équipements de vidéo-protection ou de contrôle d'accès), mais de plus en plus souvent apporter des conseils en matière de sécurité de leurs systèmes d'information.

La crise pandémique du COVID a été l'occasion de renforcer les mesures de prévention en cybersécurité et depuis le mois de mars 2020, 45000 entreprises et 12500 élus ont été sensibilisés aux risques spécifiques qu'ils pouvaient rencontrer dans ce contexte. Certaines

entreprises et collectivités locales ont été spécifiquement contactés parce qu'ils étaient plus susceptibles d'être visés par certaines attaques visant les serveurs d'accès au bureau à distance.

Pour améliorer encore cette capacité, le groupement de gendarmerie du Morbihan expérimente un nouveau dispositif intitulé « Hermès 56 ». Les gendarmes de la SOLC 56, les référents sûreté du département et les correspondants en intelligence économique expérimentent un dispositif nouveau regroupés sous cette bannière. Ils sont accompagnés par une formation développée avec l'Université de Bretagne Sud. Ensemble, ils apportent un message de prévention pluridisciplinaire auprès les collectivités locales et les entreprises du département et leurs indiquent les actions à réaliser pour une meilleure sécurisation de leur système d'information.

Ce type de dispositif départemental est progressivement étendu à l'ensemble du territoire et les SOLC relaient en particulier les messages de l'ANSSI et de Cybermaillance.gouv.fr et en deviennent les ambassadeurs.

« Le 17 septembre 2020, juste avant minuit, des impressions se lancent sur nos copieurs d'Amiens et de Nantes. Il s'agit d'un message nous indiquant que nous étions victime d'une attaque informatique et que nos données sont retenues en otage. Dès l'arrivée dès le lendemain des premiers salariés sur place, le constat est sans appel : les accès aux serveurs sont supprimés. Nous n'avons plus accès à nos données ainsi qu'aux logiciels de production. Nous avons contacté immédiatement notre prestataire informatique pour analyser la situation et restaurer les sauvegardes sur un serveur sain. Conclusion : perte sèches de deux jours de production. »

Laurent RABINEAU,
Président de la Compagnie Européenne de Travaux et d'Ingénierie

Les bons réflexes pour protéger la vie numérique des français

Les citoyennes et les citoyens participent directement au développement d'un numérique de confiance en adoptant les bons réflexes dans leurs usages au quotidien aussi bien dans la sphère professionnelle que dans la sphère personnelle.

1. Je renforce mes mots de passe pour protéger les accès à mes données personnelles et professionnelles. Besoin d'aide : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe
2. Je mets à jour mes appareils et mes logiciels dès que possible afin de ne pas devenir vulnérable face aux tentatives d'attaque.
3. Je sauvegarde régulièrement mes données dans un Cloud sécurisé et/ou sur un support externe à mon équipement.
4. Je reste vigilant dans mes usages numériques : lorsque je fais mes achats en ligne, je vérifie si le site est sécurisé. Si je reçois un message par mail ou par sms qui me semble inattendu, je vérifie par un autre moyen sa légitimité, surtout si des informations sensibles sont demandées (coordonnées bancaires, par exemple).
5. Même en télétravail, je sépare mes usages professionnels et personnels.

Contacts presse

Cabinet de Cédric O
01 53 18 43 10
presse@numerique.gouv.fr

Cabinet de Bruno Le Maire
presse.mineco@finances.gouv.fr

Secrétariat général pour l'investissement
01 42 75 64 58
presse.sgpi@pm.gouv.fr

ANSSI
06 49 21 63 80
margaux.vincent@ssi.gouv.fr