Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

La cyber résilience

Thème d'approfondissement 2017 de la section sécurité et risques

30 janvier 2018

n° 2017/02/CGE/SR

Ce rapport se présente sous un format adapté à une lecture plein écran sur un ordinateur ou une tablette. Il peut être parcouru de façon séquentielle ou « en navigant » dans le document à partir du sommaire.

CONSEIL GÉNÉRAL DE L'ÉCONOMIE
DE L'INDUSTRIE, DE L'ÉNERGIE ET DES TECHNOLOGIES

Sommaire

Cette image signale les citations directes des personnalités rencontrées ou d'acteurs de référence

Aller au sommaire

Ce rapport a été établi par les membres et chargés de mission du Conseil général de l'économie suivants (par ordre alphabétique) :

Claude CALVAYRAC, ingénieur général des mines

Yves MAGNE, administrateur civil hors classe

Marc MEYER, ingénieur général des mines, **coordonnateur de la mission**

Daniel RATIER, administrateur civil hors classe

Il a été particulièrement enrichi par les contributions de :

Serge ABITBOUL (ENS/INRIA), **Alexis CAURETTE** (ACN**), Arnaud COUSTILLIERE**(ministère de la défense),

Hervé DEBAR(IMT-Télécom Sud paris), **Thierry DELVILLE** (ministère de l'intérieur), **Philippe COTELLE** (Airbus), **Didier REMY** (INRIA)

Et par celles des ingénieurs généraux des mines, membres du conseil général de l'économie :

Christophe BOUTONNET, Mireille CAMPANA, Mario CASTELLAZZI, Serge CATOIRE, Jean CUEUGNIET, **Jean-Pierre DARDAYROL**,

Laurent de MERCEY, Dominique DRON, Philippe LOUVIAU, Philippe SCHIL, **Henri SERRES**, **Hélène SERVEILLE**, **Rémi STEINER.**

Il a bénéficié de l'apport de l'ensemble des membres de la section Sécurité et Risques du Conseil général de l'économie , présidée par

Françoise ROURE, contrôleur général économique et financier.

Aller au sommaire

Synthèse

Liste des recommandations

Les attaques dans le cyber-espace sont de plus en plus fréquentes et sophistiquées, la défense ne suffit plus à assurer la survie des organisations

Les points essentiels pour réduire les risques et les impacts

Les actions proposées

Annexes

Aller au sommaire

- 57 millions de comptes clients piratés chez UBER (2016) !
- 1 100 000 ménages victimes d'escroquerie à la carte bancaire en 2015 en France, dont 720 000 par captation des données ou débit frauduleux sur Internet !
- Le coût de l'attaque NotPetya (2017) est évalué à plus de 1 milliard d'euros au plan mondial pour les grandes entreprises, victimes « collatérales » de l'attaque subie par l'Ukraine !
- Vol de données classifiées de la National Security Agency !
- Soupçon de manipulation de l'opinion par des moyens numériques lors des élections présidentielles françaises et américaines !
- Découverte d'une « faille protocolaire » pour les transmissions WIFI (2017)
- 8000 vulnérabilités logicielles déjà connues sont identifiées dans plusieurs modèles de pacemakers commercialisés au Etats-Unis (2017)
- …

Il ne se passe pas une semaine sans qu'une nouvelle affaire nous rappelle que le cyber-espace est miné par des risques qui lui sont spécifiques. L'ampleur, la persistance et la croissance du phénomène permettent d'emblée d'écarter l'hypothèse d'un phénomène de mode médiatique nourri d'un syndrome complotiste. Chacun d'entre nous, dans son environnement proche, a déjà été témoin ou les victime de la concrétisation de la menace.

Cette nouvelle menace s'ajoute à des risques bien connus. Un grand data center subit en moyenne plusieurs interruptions de fonctionnement par mois dont un quart « seulement » est d'origine malveillante. L'impact de la plupart des catastrophes naturelles est amplifié par la destruction des moyens de communication et par l'interdépendance croissante des réseaux (communication, chaines alimentaire et sanitaire, énergie, transports …)

Le Conseil général de l'*économie*, de l'*industrie*, de *l'énergie* et des *technologies* se devait de se mobiliser sur ce sujet, c'est inscrit dans son appellation même. Le numérique est au centre de notre *économie* à l'heure de la mondialisation, de la virtualisation des échanges, de la banalisation du commerce en ligne, du déploiement des plateformes. L'*industrie* est entrée dans sa quatrième révolution, fortement liée à l'introduction massive des technologies digitales dans le cycle de production. Le secteur de l'*énergie* repose très largement sur le numérique pour l'optimisation des ressources, l'émergence des énergies alternatives et des modes de consommation qui répondront au défi climatique. Dans le même mouvement, ce secteur est une cible très exposée aux cyber-risques comme l'a montré le cas de l'Ukraine. Il partage cette situation avec plusieurs autres secteurs vitaux de l'économie : la finance, la santé, les transports. Enfin, la plupart des innovations *technologiques* actuelles (l'intelligence artificielle, les biotechnologies, la robotique, le véhicule autonome, les nanomatériaux …) sont directement liées au numérique.

Aller au sommaire

Une part croissante de nos activités s'inscrit donc dans le cyberespace pour communiquer, apprendre, consommer, se divertir, travailler, se soigner … Toutes les menaces sur cette nouvelle dimension sont donc à prendre au sérieux, quelles que soient les difficultés.

La première difficulté est le caractère relativement technique du sujet. Nous nous sommes attachés à essayer de comprendre et faire partager les principes importants cachés derrière le vocabulaire spécialisé. Cette ambition a souvent été contrecarrée par la rareté des informations fiables disponibles et celle des retours d'expérience.

La deuxième difficulté est l'amplitude du thème qui appelle à l'évidence une approche trans-disciplinaire et multidimensionnelle. Nous avons rencontré plus de cinquante interlocuteurs, lu des centaines de sources d'information et pourtant, nous restons avec le sentiment de n'avoir que partiellement traité le sujet, avec des lacunes évidentes, en particulier du côté des sciences humaines.

Nous sortons cependant de ce travail avec 3 convictions :

1 - L'important aujourd'hui est tout autant la résilience que la sécurité. Nul ne sait si la panne mondiale d'Internet est pour demain, nul ne connaît la date, la nature et l'impact de la prochaine cyber-attaque de grande ampleur mais, sans négliger les mesures de sécurité préventives indispensables, il faut se préparer dès maintenant à en gérer (et si possible maîtriser) les conséquences, quand ces mesures de défense seront débordées et inopérantes.

2 - Les principes et méthodes pour renforcer la résilience des organisations et des systèmes sont globalement connus et documentés dans l'univers du numérique. Il nous a cependant paru important d'aller questionner les approches que proposent la biologie et l'écologie pour garnir notre « trousse à outils » de « points essentiels » propres à renforcer cette résilience.

3 - La France est en très bonne place au plan mondial et européen pour la maîtrise des cyber-risques, adossée à une stratégie de l'Etat affirmée, à l'action remarquable du SGDSN et de l'ANSSI, à des entreprises solides appuyées sur une recherche de bon niveau. Mais l'objectif légitime et nécessaire de la France doit être la première place. Quand l'Europe se résout à adopter un « Paquet Cyber » faute de mettre en place une véritable « Stratégie Cyber ». Il y a une place de leader à prendre avec une urgence que dicte le principe de réalité.

C'est en tressant ces trois convictions que nous avons fabriqué le fil d'Ariane de la rédaction de ce rapport et de la formulation des recommandations qui l'accompagnent.

Nous formulons deux recommandations principales en direction de l'Etat :

- Renforcer la gouvernance interministérielle en matière de cyber résilience
- Mesurer le niveau de maturité de cyber-résilience des organisations et structurer la remontée d'information

Elles sont accompagnées de deux recommandations opérationnelles qui déclinent ces recommandations principales de façon plus précise :

- Améliorer la cyber résilience des organismes publics
- Disposer de compétences nécessaires en cybersécurité

Trois recommandations complémentaires, mais néanmoins importantes, positionnées sur des axes différents complètent le dispositif proposé :

- Faciliter l'émergence de produits et solutions innovants en matière de cybersécurité
- Mettre le numérique au service de la résilience
- Réglementer et réguler pour réduire les risques

Le cyber-espace est en crise. Allons nous vers le meilleur ou le pire est-il encore à venir ? La partie n'est pas jouée et il est encore temps. Le résultat du match dépend de chacun d'entre nous !

Synthèse

Liste des recommandations

Les attaques dans le cyber-espace sont de plus en plus fréquentes et sophistiquées, la défense ne suffit plus à assurer la survie des organisations

Les points essentiels pour réduire les risques et les impacts

Les actions proposées

Annexes

Aller au sommaire

RECOMMANDATIONS PRINCIPALES

❑ RECO 1 - Renforcer la gouvernance interministérielle en matière de cyber résilience

- Créer le conseil d'orientation de la cyber résilience (COCyR) qui a pour mission principale de formuler des recommandations régulières aux plus hautes autorités de l'Etat ainsi qu'aux secteurs de l'économie les plus concernés par la cybersécurité. Il est placé sous la responsabilité du Premier ministre,
- Mettre en place des Comités d'analyse et de partage de l'information en cybersécurité (CAPIC)pour encourager et faciliter les échanges d'informations en matière de cybersécurité entre leurs membres intervenant dans une même filière industrielle. Les filières prioritaires sont l'énergie, les finances, les transports, la santé. Le modèle des CAPIC peut être adapté aux besoins des collectivités territoriales.

❑ RECO 2 - Mesurer le niveau de maturité de cyber-résilience des organisations et structurer la remontée d'information

- Constituer un référentiel d'évaluation de la cyber résilience des organisations avec quatre déclinaisons pour :
  - Les grandes entreprises et ETI
  - Les TPE, PME, et associations.
  - Les collectivités et organismes publics, non couverts par la PSSI de l'Etat
  - Les entités publiques assujetties à la PSSIE (cf. reco N°4)
- Organiser, sur la base des remontées d'incidents enregistrées par l'ANSSI et les autres sources d'information sectorielle, la préparation d'un rapport annuel anonymisé destiné à une large diffusion permettant d'évaluer le risque cyber et de caractériser au mieux les incidents.

Aller au sommaire

RECOMMANDATIONS OPERATIONNELLES
déclinant les recommandations principales

RECO 3 - Améliorer la cyber résilience des organismes publics

- Renouveler la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) établie en 2014 afin de :
  - Procéder à la mise à jour des éléments techniques et organisationnels qu'elle doit comporter.
  - Renforcer l'implication générale des personnels de l'administration en matière de cybersécurité.
  - Doter la PSSIE d'éléments destinés à soutenir et accompagner sa mise en œuvre au profit des personnels qu'elle concerne.
  - Inclure dans la PPSIE une dimension de résilience rendue nécessaire par l'accroissement des risques et l'augmentation de la probabilité de leur occurrence.
- Auditer les ministères, organismes publics et collectivités locales, sur la base des référentiels d'évaluation de la cyber-résilience.
  - Ces évaluations devront dans un premier temps être conduite par des agents extérieurs au ministère concerné. Elles pourront par la suite être conduites par les HFDS.

RECO 4 - Disposer de compétences nécessaires en cybersécurité

- Renforcer la diffusion de la cyber-sécurité dans la formation initiale et continue, développer les formations spécifiques post-bac, en particulier au niveau technicien (UIT, BTS) et ingénieur.
- Mettre en place un dispositif de formation continue et de fidélisation associé à un label.
- Mettre en place une GPEEC des spécialistes en cyber-sécurité au sein de la sphère publique en valorisant les parcours public-privé
- Maîtriser la politique d'externalisation des ministères, en particulier dans les fonctions liées à la cybersécurité.

Aller au sommaire

RECOMMANDATIONS COMPLEMENTAIRES

❑ RECO 5 - Faciliter l'émergence de produits et solutions innovants en matière de sécurité numérique

- Mettre en place des outils pour développer des offres nationales intégrées associant monde de la recherche, grands groupes, SDN (intégrateurs) et fournisseurs de solutions, notamment des plateformes dédiées à des usages de sécurité .
- Concentrer sur ces plateformes l'expérimentation de solutions innovantes intégrant la dimension « privacy by design » et les études d'impact liées au RGPD afin de développer des offres de solutions françaises exportables qui intègrent les obligations de ce règlement .
- Mutualiser les comités d'analyse, d'expertise et de décision pour l'attribution des aides publiques dans le domaine de la cybersécurité (ANR, FUI, RAPID).

❑ RECO 6 - Mettre le numérique au service de la résilience

- Mobiliser les ressources numériques et les communautés pour accompagner la gestion de crise : communications mobiles, réseaux sociaux (associations RAND, VISOV), voire développer par anticipation des ressources locales autonomes (réseaux électriques locaux, communications satellitaires…) .
- A l'instar de la Direction générale de sécurité civile et de la gestion des crises (DGSCGC) qui a mis en place un système de conventions avec des associations de proximité telles que VISOV, il s'agit de mobiliser les communautés de volontaires de proximité avec pour objectif de compléter le dispositif de remontée des alertes par la détection d'évènements hors voies traditionnelles.

❑ RECO 7 - Réglementer et réguler pour réduire les risques

- Intégrer dans l'économie numérique le principe de responsabilité des fournisseurs systémiques de dispositifs numériques (hard ou soft) connectables. Supprimer ou restreindre l'exception du numérique dans ce domaine.
- Pour favoriser l'assurabilité du risque cyber , mettre en place un dispositif de co-working entre assureurs, commissaires aux comptes, acteurs privés et puissance publique pour renforcer l'offre du marché de l'assurance de la cyber sécurité.

NB : d'autres suggestions, plus secondaires ou relevant de simples pistes de réflexion, figurent dans le texte du rapport, signalées par une flèche ➡

Aller au sommaire

Synthèse

Liste des recommandations

Les attaques dans le cyber-espace sont de plus en plus fréquentes et sophistiquées, la défense ne suffit plus à assurer la survie des organisations

Les points essentiels pour réduire les risques et les impacts

Les actions proposées

Annexes

Aller au sommaire

Les attaques dans le cyber-espace sont de plus en plus fréquentes et sophistiquées, la défense ne suffit plus à assurer la survie des organisations

- Le cyber-espace : représentation et spécificités
- L'attribution des cyber-attaques reste incertaine et cela pénalise la mesure des effets des pannes ou des prédations
- Risques et menaces cyber : catégories de prédateurs et faiblesse des systèmes face aux pannes et aux attaques

Aller au sommaire

Le cyber-espace : représentation et spécificités

Il n'existe pas de définition officielle et universellement reconnue du cyber-espace. L'ANSSI propose dans son glossaire en ligne : «Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques. ». Le cyber-espace apparaît plus englobant et plus étendu qu'internet, lequel est indispensable à son existence de par l'interconnexion des réseaux qui le constituent.

Le cyber-espace peut être vu selon au moins trois dimensions :

- une dimension matérielle, celle des réseaux, Internet au premier rang mais aussi les réseaux professionnels comme les réseaux bancaires et maintenant les réseaux à bas débit qui constituent l'internet des objets ; ensuite les artefacts de plus en plus nombreux et de plus en plus complexes qui sont intégrés et même composants du cyber-espace : machines et usines, équipements médicaux puis hôpitaux et systèmes de soins, etc ;
- une dimension logique relative à l'ensemble des applications de tous types ;
- une dimension sémantique, comprenant évidemment les informations de toutes sortes mais aussi leurs structurations plus ou moins formelles, des méta-données au sens classique jusqu'aux réseaux sociaux en passant par les processus et les règles d'affaires qui structurent les entreprises, les organisations, les activités sociales et économiques .

Le cyberespace est perçu comme un facteur de risques et de menaces et comme un champ de confrontation. Suite à l'intensification des attaques informatiques visant les Etats, ces derniers ont identifié la cyber-menace comme relevant d'une question de sécurité nationale.

En regard d'autres domaines soumis à différentes formes de risques, l'insécurité qui concerne le cyberespace présente des caractéristiques qui rendent sa gestion particulièrement difficile.

L'attribution d'une attaque demeure le plus souvent incertaine. La difficulté à connaitre l'attaquant et les raisons qui le poussent à agir est t aggravée par l'évolution permanente des technologies du numérique qui crée tout aussi régulièrement de nouvelles opportunités d'agression. Les dynamiques spécifiques du cyber espace donnent un avantage permanent à l'attaquant qui, tout en restant masqué, peut utiliser des techniques et des méthodes innovantes encore inconnues du défenseur. Ce dernier n'étant pas en mesure de prévoir les auteurs, les raisons et les modalités de l'attaque dont il va faire l'objet, sa capacité à y faire face s'en trouve réduite d'autant.

Ces incertitudes altèrent également la mesure des effets des prédations. Les estimations sur le sujet ont en commun d'avancer des ordres de grandeur particulièrement élevés, et des chiffres approximatifs. Les méthodes de calcul pour évaluer les pertes des entreprises attaquées aboutissent presque systématiquement à une sous-évaluation et leurs comptes sur le sujet sont très rarement publics. Ces incertitudes pèsent sur l'évaluation de l'investissement nécessaire à la cyber-sécurité, que ce soit au niveau des Etats, des secteurs de l'économie ou des entreprises. Il n'existe actuellement pas d'évaluation précise permettant de connaître le montant de l'effort économique souhaitable pour se protéger des cyberattaques.

Ces difficultés atteignent un niveau critique dans un contexte marqué par la transformation numérique qui touche en particulier les entreprises, les particuliers, les systèmes ainsi que la plupart des organisations. Les effets associés de la forte croissance de la dépendance au numérique et de l'insécurité dans le cyberespace doivent faire l'objet d'un effort prioritaire pour en limiter les risques et leurs conséquences.

Les handicaps de la défense évoqués précédemment, qu'ils soient du domaine de la cyber-sécurité, qui concerne habituellement le monde des entreprises et l'économie, ou de la cyberdéfense qui relève des Etats, constituent des caractéristiques spécifiques du cyberespace que l'on ne trouve pas dans d'autres contextes stratégiques. Dans la complexité et l'obscurité du cyberespace en mouvement permanent, Il est maintenant confirmé que les stratégies classiques de défense ne peuvent faire face à l'intensité de la montée des risques qui touchent des sociétés toujours plus dépendantes du numérique. Une alternative stratégique apparait donc nécessaire. Ce besoin a justifié le développement du concept de cyber-résilience dont les premières évocations remontent au World Economic Forum de Davos en 2012, dans la publication «Partnering for Cyber Resilience », sous la houlette du cabinet Deloitte.

Cette publication introduisait le concept de cyber-résilience en proposant également des définitions des concepts de cyber-sécurité, de risques cyber, de cyber-menaces et de vulnérabilités cyber. La cyber-résilience y était définie comme la capacité des systèmes et des organisations à résister aux événements d'origine cyber, mesurée par la combinaison du temps moyen à l'échec et du temps moyen de récupération.

Si la cyber-sécurité a pour objectif de protéger le SI de la structure, la cyber-résilience est destinée **à protéger l'activité** de la même organisation et en particulier **ses fonctions essentielles** ce qui rend nécessaire l'évaluation de leur niveau de dépendance aux risques du cyberespace.

La cyber-résilience est **une démarche globale**. Elle concerne tous les services ainsi que leurs partenaires extérieurs à la structure. Elle fait appel à tous les métiers de la structure, en particulier ceux qui concernent ses fonctions essentielles ainsi que sa sécurité et sa sûreté. Elle ne correspond pas à une démarche unique et centralisée mais plutôt à une somme de démarches spécifiques. **La résilience renvoie au systémique opposé au sectoriel.**

Le facteur humain est au cœur de la cyber-résilience. La grande majorité des évènements indésirables qui touchent le système sont d'origine humaine, involontaires et internes à la structure et un effort déterminé doit être réalisé pour en réduire l'occurrence, notamment par des opérations de communication et de formation *(réduction de l'exposition).* La cyber-résilience demande en outre des compétences techniques d'un niveau élevé au sein de l'entreprise ou à sa disposition, en particulier dans les domaines SI, cyber-sécurité, gestion de crises, métiers, sûreté, ce qui nécessite notamment une gestion adaptée des ressources humaines et financières pour prendre en compte ces besoins et si nécessaire faire appel à des spécialistes. Enfin, le traitement des problèmes et des dégâts qui suit un évènement indésirable repose souvent sur une mobilisation et un engagement du personnel de la structure, le cas échéant pour accroître la résistance à la panique, au découragement, à l'abandon.

.

Les attaques dans le cyber-espace sont de plus en plus fréquentes et sophistiquées, la défense ne suffit plus à assurer la survie des organisations

Le cyber-espace : représentation et spécificités

L'attribution des cyber-attaques reste incertaine et cela pénalise la mesure des effets des pannes ou des prédations

Risques et menaces cyber : catégories de prédateurs et faiblesse des systèmes face aux pannes et aux attaques

Aller au sommaire

L'attribution des cyber-attaques reste incertaine et cela pénalise la mesure des effets des pannes ou des prédations

- Le cyber-espace permet aux prédateurs de se dissimuler aisément et l'attribution d'une attaque demeure longue et difficile, voire incertaine, en dépit de la multiplication des services officiels et des entreprises qui s'y consacrent. La question est pourtant centrale car elle conditionne la réponse éventuelle de l'Etat dont dépend la victime, en lui permettant de déterminer le cadre juridique applicable. Quand l'attribution est possible, la désignation des coupables fait très rarement consensus en l'absence d'instance mandatée et légitime pour la valider. Les victimes, quant à elles, peinent à détecter et identifier les agressions qu'elles subissent, et se gardent souvent de les dévoiler. Les entreprises, soucieuses de leur réputation, sont généralement très discrètes à ce sujet. Les particuliers sont nombreux à ne pas détecter les fraudes dont ils sont victimes et très peu portent plainte.

- L'information ouvertement disponible sur les origines d'une attaque informatique est toujours parcellaire, quand elle existe, et d'une fiabilité incertaine car en grande partie issue de sociétés privés de cyberdéfense ou d'agences gouvernementales dont l'objectivité peut être contestée. Dans le cas de l'attaque Wannacry, aucun bilan des dégâts n'est disponible en France ou ailleurs alors qu'il est très probable que le coût de l'attaque a atteint des montants records. Europol parle de ''plus de 200 000 victimes dans au moins 150 pays''. Un Etat voyou a été désigné comme le coupable par une agence gouvernementale, la même qui s'était réservée l'utilisation de la vulnérabilité à l'origine du malware. Aucune cyberattaque n'a été revendiquée par une nation jusqu'à présent, y compris quand tout la désigne.

Aller au sommaire

Les attaques dans le cyber-espace sont de plus en plus fréquentes et sophistiquées, la défense ne suffit plus à assurer la survie des organisations

Le cyber-espace : représentation et spécificités

L'attribution des cyber-attaques reste incertaine et cela pénalise la mesure des effets des pannes ou des prédations

Risques et menaces cyber : catégories de prédateurs et faiblesse des systèmes face aux pannes et aux attaques

Aller au sommaire

Historique

Depuis leur émergence dans les années 80, les menaces cyber n'ont cessé d'évoluer, de se diversifier et de se renforcer. L'évolution permanente des technologies du numérique crée tout aussi régulièrement de nouvelles opportunités d'agressions et de pannes du fait de la complexité croissante des systèmes et de leurs interfaces. Le potentiel d'innovation qui les caractérise concerne également les techniques et méthodes des cyberattaques dont le renouvellement reste accessible à l'ensemble des acteurs du milieu, délinquants solitaires, organisations mercenaires ou criminelles, petits ou grands Etats. Ces attaquants ont l'avantage sur les défenseurs et cela devrait durer.

L'absence de super-administrateur ayant tous les pouvoirs dans la totalité du cyber-espace, en dépit de l'importance des efforts de certaines nations pour s'en assurer la maîtrise, contribue à amplifier la menace. Il n'y a pas de gendarme visible et reconnu au niveau mondial dans le cyber-espace.

Durant les décennies 80 et 90, ce sont les performances individuelles des hackers qui ont défrayé la chronique de la prédation du cyberspace. Les ''exploits'' de ces quelques codeurs solitaires ont renouvelé le mythe du David affrontant avec succès les Goliath que constituaient les grandes organisations dont les systèmes d'information avaient été pénétrés. Le sujet est embarrassant pour ces dernières mais les hackers recherchent surtout le prestige, ce qui a accru leur exposition et limité l'ampleur de leurs prédations. Certains se sont regroupés parfois pour mener des actions plus politiques que rémunératrices comme ce fut le cas lors du conflit du Kosovo en 1999. Les entreprises et les institutions sont attaquées et se défendent mais il faudra attendre la décennie suivante pour les voir passer à l'offensive.

Depuis lors, la prédation dans le cyber-espace a considérablement développé ses moyens, ses méthodes et ses organisations ainsi que sa recherche de profit. La cyber-criminalité s'est organisée, les hackers se sont mis en réseau afin de rassembler des compétences complémentaires, ils ont créé des places de marchés dans le darkweb pour acheter ou vendre des outils de hacking toujours plus sophistiqués. Certains, en particulier des Russes, proposent leurs services en mode ''Cyber-crime as a service''. Les profits qu'ils réalisent sont probablement supérieurs à ceux du trafic de drogues mais le domaine cyber n'est plus simplement un champ d'action pour les délinquants économiques.

Il est devenu un terrain privilégié pour des affrontements politiques ou même militaires. Les grandes puissances l'ont instrumentalisé en ce sens. Elles y mènent des opérations qui peuvent aboutir à des destructions dans le monde physique ou des déstabilisations politiques tout en se préparant à des cyberguerres de grande ampleur. Le cyber-espace constitue par ailleurs une base arrière médiatique, logistique et opérationnelle dont profitent les principaux mouvements du terrorisme djihadiste.

L'augmentation des cyber-menaces est la conséquence de la montée en puissance des organisations qui en sont à l'origine, qu'elles soient privées ou publiques, étatiques ou criminelles et des compétences de leurs membres. Au niveau des Etats, des pays, toujours plus nombreux, ont mis sur pied des unités dédiées à l'action offensive qui peuvent rassembler plusieurs dizaines de milliers de cyber-soldats. C'est le cas dans les trois premières nations qui ont lancé ce type de programme d'armement numérique, la Chine, les Etats-Unis et la Russie, mais on retrouve ce type d'organisation dans plusieurs pays comme l'Iran, le Royaume Uni, Israël ou la Corée du Nord qui peuvent chercher à riposter aux autres Etats. Dans ce dernier pays, on estime que l'effectif de la structure dédiée, le ''Bureau général de reconnaissance'' est passé de 500 à 600 en 2008 à près de 6000 en 2015. Cette évolution est révélatrice de l'intensité de la montée en puissance des unités de cyber-soldats. L'équivalent de la NSA en Chine compte aujourd'hui plus de 100 000 agents dont plusieurs milliers sont dédiés à des missions offensives ou d'espionnage.

Les premières cyber-attaques de nature quasi-militaire et reconnues comme telles ont été lancées en 2007 et 2008 contre l'Estonie puis la Géorgie. La concomitance avec les crises ouvertes que ces deux pays connaissaient alors avec la Russie semble mettre en cause sa responsabilité, bien qu'elle ait pour principe de ne jamais reconnaître ses actions dans le cyberespace. La technique utilisée, l'attaque par déni de service, est habituelle lors des opérations cyber à caractère politique. Elle paralysera les sites internet des gouvernements estonien et géorgien durant plusieurs jours.

Découverte en 2010, l'attaque des centrifugeuses du programme nucléaire iranien par un ver informatique nommé Stuxnet a fait date en raison de sa sophistication et des innovations qu'elle a présentées. L'opération est sortie du champ du cyber-espace puisqu'elle a permis de détruire des installations physiques en manipulant des systèmes industriels de type SCADA. Stuxnet n'est pas un virus classique, à simple action, mais une véritable cyber arme conçue sur mesure pour remplir un rôle précis. Son élaboration a fait l'objet d'un long travail préparatoire pour étudier la cible, les procédés industriels et prévoir les modes d'action les plus adaptés utilisant plusieurs failles ''zero-day'' propres à Windows ainsi que des dispositifs destinés à leurrer les antivirus. Microsoft a estimé que sa préparation avait nécessité environ 10 000 jours homme. Il a été avancé qu'elle soit issue d'une collaboration entre la NSA et les services de renseignement militaires israéliens.

L'attaque massive dont a été victime en 2012 la compagnie nationale pétrolière saoudienne Saudi Aramco est peut être la réponse iranienne à Stuxnet. Moins évoluée que cette dernière, le procédé consiste simplement à effacer les disques durs de l'adversaire, elle aboutira tout de même à mettre hors de fonction 35 000 postes de travail de la compagnie. C'est l'une des attaques les plus destructrices de l'histoire.

Pays pourtant assez réfractaire à la modernité, la Corée du Nord fait un usage étendu des différents registres des prédations du cyber-espace en démontrant la variété des possibilités auxquelles un Etat peu vertueux peut recourir. Elle s'est montrée très active en matière de cyber attaque en multipliant les agressions contre son voisin et rival du Sud. Elle a engagé différentes actions de rétorsion contre l'entreprise Sony, coupable d'avoir produit un film défavorable à son président. Elle aurait réalisé un vol pur et simple de près de 81 millions de dollars dans les caisses de la banque centrale du Bengladesh.

Si le cas de la Corée du Nord reste particulier en raison de la nature de son régime, il est pourtant susceptible d'inspirer d'autres nations. Il démontre en effet qu'un pays relativement modeste peut se doter d'une capacité suffisante pour se livrer à une large gamme d'activité de prédation dans le cyber-espace, sans qu'il soit évident d'en prouver ou même d'en détecter les méfaits.

❑ Quels sont les catégories de prédateurs du cyber-espace ?

Pour les entreprises

Les trois quarts des attaques sont réalisées par des individus extérieurs à la structure, mais un quart d'entre elles est directement imputable aux employés de cette dernière. Revanche ou vengeance sont souvent à l'origine de leurs prédations mais la plus grosse part de risque associé à des actions internes n'est pas liée à des comportements intentionnels. Une proportion très importante des agressions, proche de la moitié, est rendue possible par une organisation insuffisante de la sécurité dans l'entreprise, voire par une erreur ou un manquement à la sécurité d'un employé qui va ainsi ouvrir la voie au hacker venu de l'extérieur.

La motivation de ce dernier est avant tout économique. L'essentiel du flux des attaques est constitué d'opérations ponctuelles et ciblées, fraudes ou escroqueries, destinées à récupérer des fonds. Leurs auteurs sont des hackers indépendants de niveaux variables, agissant seuls ou en équipe d'associés et menant leurs activités sans lien en général avec les services officiels de leur pays. Les grandes entreprises des secteurs compétitifs, en particulier technologiques sont régulièrement la cible d'actions d'espionnage destinées à récupérer des données sur leurs activités et leurs produits, ou à les affaiblir. Leurs auteurs peuvent être des indépendants mais ce type d'opérations, souvent sophistiquées, reste l'apanage de services organisés d'Etat agissant dans le registre de la guerre économique qui peut également inclure des actions d'atteinte à la réputation, notamment pour le secteur des média.

Pour les administrations, services ou organismes d'état

Les attaquants sont très majoritairement des organisations dépendant d'autres Etats ou agissant en coordination avec eux. Parmi ces dernières, les ''cyber-milices'' qui réunissent des internautes pour défendre leurs causes, leurs valeurs ou leurs idéologies et qui sont bien souvent nationalistes comme ce fut le cas en Estonie en 2007 ou lors des conflits en Géorgie en 2008 ou en Ukraine. En début 2015, des ''hacktivistes'' ont piraté plusieurs milliers de sites français dont une grande proportion des sites institutionnels. Ces attaques, le plus souvent des détournements de présentation de site web, avaient été lancées en réaction à d'autres attaques réalisées par le collectif Anonymous contre des sites djihadistes après l'attentat contre Charlie Hebdo .

Compte tenu du caractère politique de leurs motivations, ces organismes d'Etat, cyber-milices et autres hacktivistes peuvent utiliser des ''cyber-armes de destruction massive'' frappant indistinctement les secteurs publics et privés ainsi que les particuliers des pays adverses. C'est le cas du malware ''Petya'' qui a récemment frappé l'Ukraine mais aussi les entreprises étrangères qui entretiennent des relations avec ce pays. Contrairement à ce qui avait été envisagé au début de sa prolifération, ce malware n'est pas un rançongiciel similaire à WannaCry, mais un logiciel destiné à détruire les installations numériques adverses.

Pour les particuliers

Ils sont le plus souvent la cible de petits escrocs utilisant des méthodes d'ingénierie sociale ou des outils de hacking disponibles sur le net. Les profits envisageables pour ce type d'activité ne justifient pas l'intérêt de hackers de haut niveau qui cibleront plutôt des entreprises. Les particuliers peuvent néanmoins faire les frais des attaques massives et indistinctes comme les récentes diffusions des malwares WannaCry ou Petya mais sans en être les cibles prioritaires. Deux autres types de risque les concernent. Les actions de cyber harcèlement ou d'atteinte à la réputation sur les réseaux sociaux qui sont en progression ces dernières années. La sensibilité forte de certaines catégories de jeunes à ce type de prédation justifie des alertes de plus en plus fréquentes de la communauté éducative des établissements scolaires au niveau collège et lycée. Autre menace qui a fait l'objet d'une intense couverture médiatique récemment, celui de la manipulation de l'information à des fins d'influence, essentiellement politique. Ce type d'activité n'est pas nouveau puisqu'il ressort de la guerre de l'information, mais les possibilités offertes par les réseaux sociaux lui donnent un pouvoir inédit et un potentiel d'industrialisation dont les ''usines à trolls'' russes ont montré l'efficacité. Il est par ailleurs difficile à tracer.

Cyber harcèlement et manipulation de l'information concernent le champ sémantique du cyber-espace. Leurs auteurs doivent donc être séparés de la catégorie des hackers habituels dont l'action cible le champ du logiciel et des données, le niveau logique du cyber-espace.

Synthèse

Liste des recommandations

Les attaques dans le cyber-espace sont de plus en plus fréquentes et sophistiquées, la défense ne suffit plus à assurer la survie des organisations

Les points essentiels pour réduire les risques et les impacts

Les actions proposées

Annexes

Aller au sommaire

❑ Cyber-résilience : Les enseignements de la biologie

Utilisé à l'origine en physique, le concept de résilience a été pour l'essentiel développé dans deux domaines. Celui de la biologie et de l'écologie où il participe au questionnement sur les écosystèmes menacés par les activités humaines, et celui de la psychologie où il constitue un phénomène permettant de dépasser un traumatisme pour revenir à un état non pathologique. D'autres domaines s'en sont également emparés, en particulier l'économie mais en s'appuyant principalement sur des modèles et des notions issus des deux premiers. Le terme de résilience est apparu dans les textes et le discours public français dans les années 2000. Le livre blanc sur la défense de 2008 en apporte une définition et l'intègre comme un élément central de la stratégie de sécurité nationale. Il correspond à une vision globalisée de la sécurité qui met en évidence les interdépendances des institutions, de la société et de la vie économique et se définit comme ''*la volonté et la capacité à résister aux conséquences d'une agression ou d'une catastrophe majeures, puis à rétablir rapidement leur capacité de fonctionner normalement, ou à tout le moins dans un mode socialement acceptable*.'' Cette présentation confirme l'opportunité du recours à la notion de résilience en biologie dont elle prend en compte la dimension systémique et la nécessité de coopération. Elle incite à utiliser la même référence comme grille d'analyse destinée à une exploration empirique des postures face aux risques et menaces du cyberespace et de leurs conséquences.

En biologie, la vulnérabilité d'un système associe une composante externe, son exposition, assez comparable à la notion de menace qu'utilisent les stratèges militaires, à deux composantes intrinsèques, sa sensibilité et sa capacité de réponse qui décrit son aptitude à s'ajuster, par exemple, en réduisant l'impact des dommages subis. La capacité d'un système à réparer des dégâts qu'il subit fait partie de sa capacité de réponse. L'exposition dépend de la fréquence et de l'ampleur avec lesquelles le système est soumis à des perturbations extérieures. La sensibilité est le degré auquel il va répondre à une sollicitation même faible.

La protection des écosystèmes naturels, qu'elle soit liée aux mécanismes internes de ces écosystèmes ou à l'intervention humaine, dans le cas de l'agriculture ou de la préservation du patrimoine naturel, par exemple, s'appuie sur quatre règles particulières : **distinguer, séparer, alterner et tracer.**

Dans le champ du cyber et en accord avec la définition de la résilience issue de la biologie, cette dernière ne se réduit pas à l'antithèse de la vulnérabilité qui, en l'occurrence, peut être liée aux attaques. Tout d'abord parce qu'elle prend en compte des perturbations qui ne sont pas du registre de la prédation d'origine humaine, comme les catastrophes naturelles, les accidents ou les pannes, mais également car la résilience se fonde sur des principes dont la portée dépasse largement les notions habituelles de sécurité ou de vulnérabilité.

Aller au sommaire

❑ Des constats issus de la biologie et de l'écologie

La résilience renvoie au systémique opposé au sectoriel et doit se concevoir à une échelle globale, en raison des interdépendances au sein des écosystèmes et entre les écosystèmes eux mêmes. Cette réalité de l'écologie concerne également le champ du cyber pour les mêmes raisons.

La coopération, opposée à la compétition, participe au potentiel de résilience. D'un point de vue biologique, la concurrence et le conflit sont en général plus coûteux en énergie et plus risqués que la coopération, pour un individu ou un groupe, comme ils le sont pour une société. C'est également le cas dans le domaine de la cybersécurité où les déficits de coopération, en particulier internationaux, et la concurrence entre les entreprises qu'il rassemble participe à l'obscurité qui le caractérise et font obstacle à la sécurisation.

La résilience ne va pas de pair avec la performance. En situation perturbée, la priorité va à la redondance, à la stabilité en mode dégradé, à la capacité multitâches en coopération qui deviennent plus importantes que la performance de chacune des parties du système.

La résilience est indissociable d'une notion de durée sur le long terme. La valeur de son potentiel ne sera pas uniquement liée à l'ampleur des perturbations auxquelles elle permettra de faire face mais aussi à leur nombre et à l'intensité de leur enchaînement. Elle constitue donc une posture particulièrement adaptée aux aléas du cyberespace, marqué par une forte progression des prédations et, avant tout, par un mouvement permanent d'expansion et d'innovation qui laisse peu d'espoir de stabilité à court ou moyen terme. La résilience n'est pas seulement une affaire de robustesse et de plasticité, elle doit également incorporer une dynamique des transformations nécessaires à la conservation des fonctions essentielles des structures qu'elle concerne.

Aller au sommaire

Les points essentiels pour réduire les risques et les impacts

❑ Des principes adaptables au monde numérique

Dans l'écosystème du numérique, la transposition des quatre principes, distinguer, séparer, alterner et tracer, peut aboutir aux indications suivantes :

distinguer

- S'inspirer de l'analyse des risques de type Seveso lors du développement de systèmes d'information.
- Hiérarchiser les sphères d'enjeux au sein du système d'information : disponibilité, intégrité, confidentialité, fiabilité.

séparer

- Utiliser les méthodes destinées à la ''Security by design '' pour l'architecture
- Séparation volumétrique/qualitative pour faciliter la cartographie du SI
- Compartimenter le SI pour éviter les systèmes ''millefeuilles''
- Séparation physique et/ou virtuelle pour le stockage des données, le Cloud
- Prudence et vigilance à propos du BYOD et de l'IoT
- Mieux gérer le cycle de vie et l'obsolescence du SI et de ses outils
- Investir pour diminuer la dette technique

alterner

Prévoir des **redondances** :

- Physiques (back up)
- Logiques (codages différents) ?
- Technologiques (non numériques ?)

tracer

Effort sur la traçabilité :
Normer ses éléments constitutifs et y intégrer ceux de la sécurité.

- Effort sur la qualité du code (IoT en particulier)
- Ouverture du code
- Ouverture des données
- Mise en œuvre de l'identité numérique

Aller au sommaire

Les points essentiels pour réduire les risques et les impacts

- Anticiper
- Réduire les vulnérabilités
- Distinguer et séparer
- Alterner
- Tracer
- Synthèse

❑ Décloisonner la question de la cyber-sécurité pour renforcer la résilience par une approche multidisciplinaire de la gestion du risque cyber en sortant d'un traitement trop exclusivement technique et / ou trop numérique.

Depuis les années 90, les types de risque cyber se sont multipliés en association avec de nombreuses formes de prédation différentes. Si certaines d'entre elles passent par des montages techniques toujours plus évolués comme par exemple les ''advanced persistent threat (APT)'', d'autres nécessitent des compétences différentes, dans le registre de l'influence, de la manipulation de l'information, de l'ingénierie sociale. Dans certains cas, les connaissances requises pour les attaquants sont bien davantage liées aux contexte de l'attaque, aux métiers qu'elle cible plutôt qu'à des questions techniques.

La nature de la menace s'est donc diversifiée. Cela nécessite que sa prise en compte le soit également, en sortant du techno-centrisme qui prévaut dans ce domaine.

Une telle évolution est d'autant plus indispensable que la protection offerte par la cybersécurité n'est aujourd'hui plus suffisante. Il est en effet admis que certaines attaques évoluées ne pourront être contrecarrées, et qu'il faut donc se préparer à subir des dommages. Ce constat, qui fonde la cyber-résilience, engage en particulier à porter un regard plus précis sur les conséquences des attaques et des prédations afin d'en limiter l'ampleur et permettre la récupération. Pour y parvenir, les compétences nécessaires ne sont pas celles du champ technique habituel de la cybersécurité mais relèvent plutôt de la gestion du risque, de problématiques économiques, de domaines liés au facteur humain.

❑ Faire remonter l'exigence de sécurité dans les arbitrages sur le système digital au niveau technique, ressources humaines et gouvernance

Les questions de cybersécurité sont le plus généralement discutées au niveau technique, au sein des DSI, par ceux qui en ont la charge et les responsables du SI. Il faut généralement un problème grave pour que le débat sorte de ce cénacle.

L'importance des enjeux associés à la prédation dans le cyberespace et à ses conséquences pour les organisations, qu'elles soient publiques ou privées, doivent inciter à mettre en place une gouvernance plus proche des niveaux décisionnels.

❑ Intégrer la sécurité dès la phase de conception des architectures et des applications (« security by design »)

Il est toujours beaucoup plus coûteux et hasardeux d'ajouter, après coup, des parades sur un système d'information que de concevoir dès l'origine des systèmes résilients, même si cela représente un coût immédiat, tant en ressources à mobiliser qu'en délai de mise à disposition des applications. Pressées par le temps et la concurrence, de nombreuses starts-up, mais pas seulement, font l'impasse sur la sécurité pour livrer leurs produits dans des délais les plus rapides possible, c'est parfois même une question de survie de l'entreprise. L'administration fait aussi cet arbitrage, le plus souvent pour des questions budgétaires, accumulant ainsi une « dette technique sécurité SI » dont elle aura à payer le prix dans les années suivantes.

Les points essentiels pour réduire les risques et les impacts

- Anticiper
- **Réduire les vulnérabilités**
- Distinguer et séparer
- Alterner
- Tracer
- Synthèse

Aller au sommaire

❑ Décider ce qui doit être impérativement protégé au sein de la structure

Il est très important, quand on considère la cyber-sécurité et la cyber-résilience d'une entreprise donnée ou d'un système donné, de se demander quels sont les enjeux prioritaires :

1. La disponibilité : le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

2.L'intégrité : les données doivent être celles que l'on attend et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets.

3.La confidentialité : seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

A titre d'illustration, le SI de l'INSEE est plus sensible à la confidentialité et dans une moindre mesure à la disponibilité, alors que le SI de la RATP serait bien plus sensible à la disponibilité et à l'intégrité qu'à la confidentialité.

Il est donc essentiel d'adapter la gouvernance des SI aux enjeux de la sécurité des systèmes et des données selon ces critères stratégiques.

❑ Encourager les démarches de type PCA et PRA

Les plans de continuité d'activité (PCA) comprennent une partie métier et une partie système d'information qui devraient être étroitement imbriquées, mais ce n'est malheureusement pas souvent le cas. Si des plans de back-up de l'informatique sont souvent établis, ils sont aussi souvent menés indépendamment des plans de reprise d'activité (PRA) métier. De plus, il est assez rare de constater l'existence de plans de continuité d'activité pour un processus métier complet impliquant plusieurs ministères ou directions, ce qui est pourtant le cas général. Enfin, quand ils existent, les PCA et les PRA ne sont pas mis à jour régulièrement.

❑ Maîtriser l'externalisation en particulier pour la cyber-protection

Trop souvent, l'externalisation est subie et sert surtout à pallier le manque de moyens en interne. Or, il est certain que l'on ne sous-traite bien que ce que l'on comprend. De plus, il est important de ne pas sous-traiter ce qui fait le cœur de métier de l'organisation. On constate assez fréquemment que ni le taux ni la nature de sous-traitance ne font l'objet d'une stratégie explicite. Compte tenu des risques associés aux cyber-attaques ou aux catastrophes impliquant des interruptions du SI (incendies ou évènements météo graves), il semble essentiel que la maîtrise de la cyber-sécurité et au-delà de la résilience de l'organisation soient assurée en interne.

❑ Mobiliser décideurs, managers et ingénieurs sur le risque sémantique (manipulation, réputation, démocratie)

Les risques associés aux vulnérabilités cyber sont trop souvent appréciés sur les plans technique (niveau infrastructure) et fonctionnel (niveau traitement) qui sont, historiquement les plus fréquents. Cependant, on voit de plus en plus émerger des attaques ciblées sur une troisième dimension : les contenus « sémantiques ». Ainsi, on voit apparaître des attaques ayant pour but de nuire à une organisation, en particulier en attaquant sa réputation (défiguration de sites, par exemple), ou de manipuler l'opinion, mettant en péril jusqu'aux principes mêmes de la démocratie, comme on a pu le voir lors de récentes élections. Si la désinformation ne date pas d'aujourd'hui, les moyens mis en œuvre dans le cyber-espace la font passer à une toute autre échelle de temps et d'espace. Or les décideurs et les ingénieurs qui conçoivent les systèmes sont parfois peu sensibilisés à cette dimension sémantique mettant en risque l'entreprise ou l'Etat de droit.

Les points essentiels pour réduire les risques et les impacts

Aller au sommaire

❑ Introduire une matrice des risques dans la cartographie du SI

La démarche d'élaboration de matrice des risques est le point de départ de tout plan de continuité d'activité mené dans les règles de l'art. Force est de constater que cette analyse n'est pas toujours menée lors de développements applicatifs nouveaux, induisant de ce fait des risques sur les métiers, en particulier lorsque les processus métiers sont transverses, ce qui est un cas de plus en plus fréquent.

❑ Compartimenter le SI pour réduire le risque de propagation/contagion

On a longtemps raisonné dans le sens de l'ouverture des systèmes, combattu les « silos », créé des systèmes intégrés et des interfaces ouvertes avec les systèmes collatéraux. L'objectif recherché est de réaliser un maximum d'économies, sans rupture de continuité et donc sans intervention humaine en cours de processus. Malheureusement, il faut bien admettre que de tels systèmes portent en leur sein le germe de la propagation des « virus » informatiques, permettent aux hackers de pénétrer aisément un système en passant par un autre. Il faut donc reconsidérer cette approche et envisager, pour les systèmes les plus sensibles, une séparation nette au niveau des interface, tout en préservant au mieux l'inter-opérabilité.

❑ Aborder tous les facteurs de risques, y compris les BYOD, Objets connectés, mobilité.

De plus en plus fréquemment, les utilisateurs ont la possibilité d'utiliser le terminal de leur choix, pourvu qu'il respecte certaines règles techniques de base. Cette tendance est renforcée avec le développement du travail en mobilité, mais aussi par le fait que les outils privés sont bien souvent plus performants que ce que peut fournir l'entreprise. Il est donc devenu peu supportable d'avoir une ergonomie dégradée sur son lieu de travail. Cette tendance va en croissant et induit bien sur une fragilité supplémentaire due à la diversité des terminaux en question et à la difficulté de maîtriser le parc installé potentiel.

Comme a pu le mettre en lumière l'attaque en déni de service d'OVH (attaque dite MIRAIL, fin 2016), les objets connectés sont devenus eux aussi des relais ou des outils à disposition des hackers. Or ils sont de plus en plus nombreux, assez peu protégés et difficiles à mettre à niveau. Là aussi la croissance de tels objets est exponentielle, et n'est pas prête à diminuer.

❑ Gérer le cycle de vie (et l'obsolescence) du SI et de ses outils

Un système d'information de grande organisation est constitué de «couches archéologiques » hétérogènes, peu documentées pour les plus anciennes, et conçues à une époque où les problèmes de sécurité et de résilience étaient très loin d'être aussi prégnants qu'aujourd'hui. Les logiciels les plus anciens sont aussi ceux qui sont le plus au cœur des processus métier. Bien souvent, personne n'ose y toucher pour toutes ces raisons, et toute modification est en général très coûteuse, parfois hasardeuse. La gestion de l'obsolescence du SI est donc un enjeu de taille et elle conditionne le degré de sécurité associé. Pour y remédier, dans les systèmes nouveaux, il est urgent de mettre en place une gestion rigoureuse du cycle de vie complet des applications et des infrastructures, y compris leur suppression.

❑ Investir pour diminuer la dette technique

La pression des métiers pour disposer de nouvelles fonctionnalités est très importante, les ressources sont donc en priorité affectées aux nouveaux développements, sans vraiment dégager celles qui sont induites en MCO (maintien en condition opérationnelle). L'exploitation est donc le « parent pauvre », et la mise à niveau de la sécurité en fait partie. Wanacry s'est déployé sur des systèmes dont la mise à jour avait été différée. Il est donc important d'investir sur la mise à niveau des systèmes au même titre que sur les systèmes nouveaux.

Les points essentiels pour réduire les risques et les impacts

- Anticiper
- Réduire les vulnérabilités
- Distinguer et séparer
- **Alterner**
- Tracer
- Synthèse

Aller au sommaire

❑ S'assurer que les systèmes de back up sont efficients et à jour dans la cadre de PRA

Il ne suffit pas d'avoir un plan de back up de système d'information, il faut le tester régulièrement, et également en tester la validité dans le cadre des plans de continuité de service et de reprise d'activité, donc avec le concours des métiers. De tels tests sont exécutés dans le cadre d'opérations « piranet » sur les systèmes d'information vitaux pour l'administration, en complément du plan de vigilance, de prévention et de protection Vigipirate. Néanmoins, ces tests de garantissent pas la reprise d'activité sur back up en cas d'indisponibilité du SI.

❑ Développer des systèmes redondants et envisager la redondance du code

La redondance des systèmes est une solution connue en termes de cybersécurité. En fonction de la criticité des systèmes, plusieurs options sont possibles : redondance des disques durs, notamment en répartissant les données sur un ensemble de disques durs organisés en grappe, redondance des serveurs en utilisant la réplication en temps réel des données entre deux serveurs, redondance multi-site en répartissant les sauvegardes sur plusieurs sites.

Un autre type de redondance mériterait d'être étudié. Il s'agit de celle qui peut concerner des applications critiques développées à partir de codes différents.

La redondance peut également s'appliquer au réseau, en prévoyant par exemple le doublement d'une connexion WIFI par un réseau fixe.

❑ Quand c'est envisageable, conserver des processus « non numériques » pour maintenir un service minimum en période de crise

La tendance au ''tout numérique'' ne doit pas aboutir à renoncer aux possibilités alternatives quand la criticité des systèmes le justifie ou quand des solutions non numériques sont accessibles. Dans les centrales nucléaires, par exemple, des doubles commandes analogiques de secours sont mises en place.

Néanmoins, revenir à des procédures manuelles en cas d'indisponibilité du SI, est souvent très difficile dans la durée du fait du manque de personnel ou de contraintes matérielles d'organisation.

Les points essentiels pour réduire les risques et les impacts

- Anticiper
- Réduire les vulnérabilités
- Distinguer et séparer
- Alterner
- **Tracer**
- Synthèse

Aller au sommaire

❑ Disposer des dispositifs (hard et soft) pour expertiser les dysfonctionnements

La plupart des systèmes fournissent des traces détaillées de leur fonctionnement (journaux, logs …). La difficulté majeure, qui doit être anticipée, est de disposer des outils et des compétences permettant d'analyser ces traces. Ces études sont souvent facilitées par le maintien d'environnements de test permettant de «rejouer » les événements constatés sur les systèmes en production .

❑ Faire remonter les informations sur les cyber incidents sur la base d'indicateurs labellisés.

Comme on l'a vu précédemment, le cyber-espace permet une dissimulation propice aux prédations qui s'y déroulent. La mise en place de processus de reporting destinés aux victimes constitue donc une recommandation essentielle bien que délicate à mettre en œuvre.

Elle parait indispensable pour parvenir à établir la résilience qui s'appuie en particulier sur la capacité des systèmes à tirer parti des agressions qu'ils subissent dans une optique d'amélioration continue des défenses qu'ils mettent en place.

Il n'existe pas de reporting unifié et consolidé. Au contraire, une multitude d'intervenants tendent à instituer leur format de reporting (ANSSI, BCE, directive DSP2, directive network infrastructure security, CNIL, ...) sans cohérence. Nous ne disposons actuellement que de très peu de mesures des cyberattaques.

Alors que le Comité de Bâle avait institué dès 2004 (Bâle II) une méthodologie d'analyse du risque opérationnel et tendait à obliger les banques à calculer un plancher de fonds propres à partir d'un recensement, d'une catégorisation et d'une modélisation des risques (cf. International Convergence of Capital Measurement and Capital Standards, A Revised Framework, http://www.bis.org/publ/bcbs128.pdf), l'ACPR ne semble pas disposer aujourd'hui de la part des banques d'informations claires sur les pertes avérées et sur les incidents qui auraient pu conduire à une perte ("near-miss").

***Marc ANDRIES**, délégation au contrôle sur place à la Banque de France*

❑ Rendre les systèmes transparents, exploiter le potentiel du logiciel open source, ouvrir les données

La question des vertus de la transparence en matière de cybersécurité parait incontournable mais elle doit être abordée avec prudence et pragmatisme.

En cryptologie, la sécurité par l'obscurité va à l'encontre du principe de Kerckhoffs (1983) qui veut que la sécurité de tout cryptosystème ne doit reposer que sur le secret de la clé, les autres paramètres étant supposés publiquement connus. La mise en cause de la sécurité par l'obscurité a pu être étendue à la question du code des logiciels. Elle repose sur l'idée que le code source étant public et donc auditable, la sécurité des logiciels libres peut être mieux assurée. Pour autant, ce type de logiciel est loin d'être invulnérable puisqu'il connait également des failles de sécurité exploitables dont certaines n'ont parfois été détectées que tardivement (cas de la faille Heartbleed par exemple). Il semble probable que les avantages d'un logiciel open source en matière de sécurité sont étroitement dépendants de la vigilance de la communauté qui le produit et de sa réactivité quand une faille est détectée. Dès lors, ces avantages ne peuvent être évalués qu'au cas par cas.

Il est par ailleurs évident que la transparence de la cartographie d'un SI présente le risque de faciliter la tâche à des agresseurs potentiels, en particulier si leur niveau technique est élevé.

Pour ce qui concerne les données, l'ouverture dont elles peuvent faire l'objet peut généralement apporter une certaine sécurité quant à leur intégrité, dès lors que ces données n'ont pas un caractère confidentiel.

❑ Approfondir la question de l'identité numérique et de la signature numérique

L'identité numérique peut être divisée en trois catégories :

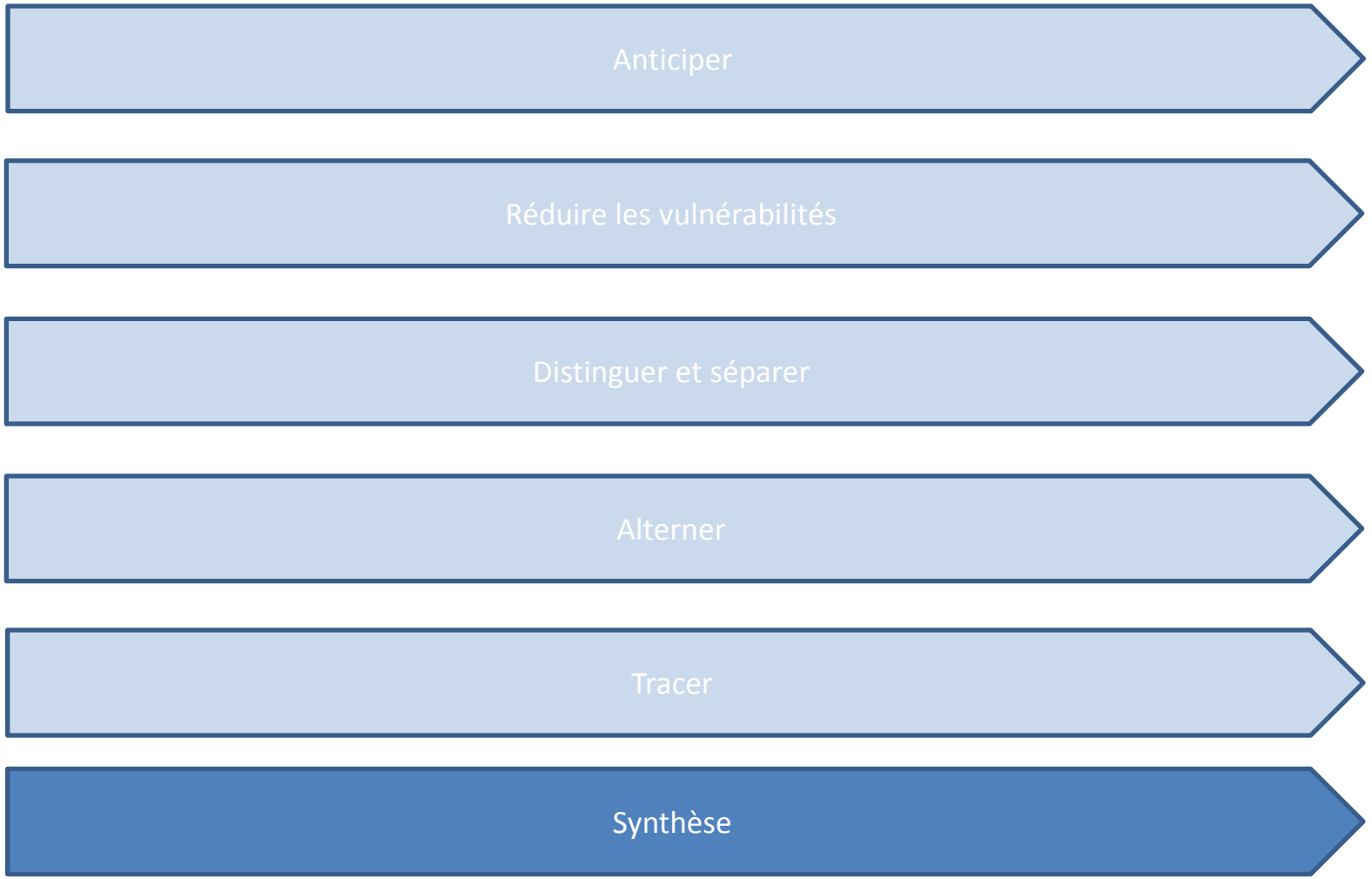
- l'identité déclarative, qui se réfère aux données saisies par l'utilisateur comme son nom, sa date de naissance, ou autres informations personnelles directement renseignées par l'individu ;
- l'identité agissante, qui est indirectement renseignée par les activités de l'utilisateur sur la toile ;
- l'identité calculée , qui résulte d'une analyse de l'identité agissante par le système.

L'identité déclarative, à laquelle peut être associée une signature numérique, peut être considérée comme un moyen efficace pour préserver les identités et valoriser les droits dans un environnement digital.

Elle permet en effet d'optimiser et renforcer la protection des accès aux sites physiques et logiques ainsi qu'aux données, d'assurer la traçabilité et l'imputabilité des actions, de respecter des réglementations et des normes exigeantes tout en favorisant la dématérialisation sécurisée des échanges.

Ces avantages sont cependant contrecarrés par les risques d'usurpation de cette identité, qui sont en forte augmentation, ainsi que les menaces éventuelles sur la liberté d'expression si cette identité peut être associée à l'identité agissante ou calculée.

Les points essentiels pour réduire les risques et les impacts



Aller au sommaire

Cyber-résilience – Points essentiels

Dispositions techniques et organisationnelles destinées à la cyber-résilience pour réduire les vulnérabilités

Réduire la sensibilité aux perturbations et les dépendances
Rendre plus robuste face à l'adversité du numérique

Décider de ce qui doit être impérativement protégé au sein de la structure
Quelles sont les fonctions métier s qui font sa raison d'être ?

Décloisonner la question de la cyber-sécurité pour renforcer la résilience
- Par une approche multidisciplinaire de la gestion du risque cyber
- En sortant d'un traitement trop exclusivement technique et / ou trop numérique

Adapter la gouvernance des SI aux enjeux de la sécurité des systèmes et des données (disponibilité, intégrité, fiabilité)

Faire remonter l'exigence de sécurité dans les arbitrages concernant le système numérique, sur les plans technique, ressources humaines et gouvernance

Maîtriser l'externalisation, en particulier pour la cybersécurité

Former et mobiliser les décideurs, les managers et les personnels sur le risque sémantique (manipulation, réputation, démocratie)

Encourager les démarches de type PCA et PRA
PCA : Plan de continuité d'activité
PRA : Plan de reprise d'activité

Adopter les principes généraux issus de la biosphère

Distinguer et séparer

- **S'inspirer de l'analyse des risques de type Seveso** lors de la production de SI - Hiérarchisation des sphères d'enjeux
- **Développer systématiquement une approche « security by design »** pour l'architecture et le codage
- **Introduire une matrice des risques** dans la cartographie du SI
- **Compartimenter le SI** pour réduire le risque de propagation des attaques
- **Séparer, au niveau physique et virtuel, les différents éléments du SI** (infrastructures, code, données) -> Cloud, virtualisation …
- **Traiter tous les facteurs de risques**, y compris les BYOD (Bring Your Own Device), les objets connectés, la mobilité
- **Gérer le cycle de vie** et l'obsolescence du SI et de ses outils
- **Investir pour diminuer la « dette technique »**

Alterner

- **S'assurer que les systèmes de back up sont effectivement déployés**, à jour et opérationnels, en particulier dans la cadre d'exercices de mise en œuvre de PRA
- **Développer des systèmes alternatifs** (codages différents) pour les systèmes les plus critiques
- Quand c'est envisageable, **conserver des processus « non numériques »** pour maintenir un service minimum en cas de crise majeure

Tracer

- Déployer les dispositifs (traces logicielles, environnements de tests …) permettant d'expertiser les dysfonctionnements en cas de crise
- Faire remonter les informations sur les cyber incidents sur une base d'indicateurs labellisés
- Rendre plus transparents les systèmes, exploiter le potentiel du logiciel open source, ouvrir les données
- Approfondir la question de l'identité numérique

Aller au sommaire

Synthèse

Liste des recommandations

Les attaques dans le cyber-espace sont de plus en plus fréquentes et sophistiquées, la défense ne suffit plus à assurer la survie des organisations

Les points essentiels pour réduire les risques et les impacts

Les actions proposées

Annexes

Aller au sommaire

- Renforcer la gouvernance interministérielle en matière de cyber résilience
- Mesurer le niveau de maturité de cyber résilience des organisations, structurer la remontée d'information
- Améliorer la cyber résilience des organismes publics
- Disposer de compétences nécessaires en cybersécurité
- Faciliter l'émergence de produits et solutions innovants en matière de cybersécurité
- Mettre le numérique au service de la résilience
- Réglementer et réguler pour réduire les risques

Aller au sommaire

Pour faire face à des menaces grandissantes, le dispositif de l'Etat destiné à la cybersécurité a fait l'objet d'un effort important dans le domaine de l'expertise technique. Une telle orientation était indispensable pour identifier et comprendre les menaces afin de pouvoir les réduire. Le développement de ces compétences et leur internalisation a permis de parvenir à un niveau élevé dans ce domaine. Il constitue un atout pour notre pays, en particulier parmi les autres nations de l'UE. La gouvernance de ce dispositif a donc été prise en charge par l'expertise technique, en cohérence avec l'axe d'effort prioritaire. Cette posture peut cependant trouver ses limites actuellement en raison de la diversification des menaces dont la dimension technique n'est plus toujours aussi centrale.

Aujourd'hui, le risque sémantique est devenu une préoccupation prioritaire pour les Etats. S'il est associé à la manipulation de l'information dont les réseaux sociaux démultiplient l'efficacité, il ne s'appuie pas sur une performance particulière de ces derniers mais simplement sur le détournement de leur usage. Dans le registre économique, la prédation rendue possible par le numérique a également vu son impact progresser très fortement avec des conséquences toujours plus lourdes pour les entreprises. Elle est cependant souvent associée à des opérations d'intelligence économique qui peuvent combiner le renseignement, le ''social engineering'', la manipulation de l'information. Dans tous les cas cas, la question technique ne constitue qu'un des aspects d'opérations qui engagent également d'autres méthodes.

On peut également constater que les problématiques de sécurité du cyberespace ont tendance à sortir du champ régalien traditionnel. C'est particulièrement le cas dans le domaine économique où la prédation s'est intensément développée et constitue une menace permanente pour les entreprises, grandes et petites.

Ces évolutions incitent à envisager une gouvernance du dispositif de l'Etat moins focalisée sur les aspects techniques et plus ouverte sur des compétences correspondants à des champs qui peuvent participer à la résilience générale de notre pays face aux menaces issues du cyberespace.

Elle doit en particulier inclure des acteurs économiques parmi les plus concernés par les cyber menaces, que ce soit parmi ceux qui y sont particulièrement exposés ou ceux qui peuvent contribuer à s'en protéger.

Une telle gouvernance doit donc associer les acteurs publics et privés.

Recommandation N° 1 - Renforcer la gouvernance interministérielle en matière de cyber résilience - (1/2)

Action 1 : créer le conseil d'orientation de la cyber résilience (COCyR)

❑ Objectifs et modalités

Ce conseil a pour mission principale de formuler des recommandations régulières aux plus hautes autorités de l'Etat ainsi qu'aux secteurs de l'économie les plus concernés par la cybersécurité.

Il est placé sous la responsabilité du Premier ministre,

Le COCyR s'appuie sur une représentation forte du secteur privé, issue à la fois des entreprises productrices de services ou dispositifs destinés à la cyber-sécurité et de celles qui sont exposées au risque cyber dans le cadre de leurs activités.

Il rassemble des représentants des collectivités territoriales, des parlementaires nationaux et européens ainsi que des personnalités qualifiées notamment issues du secteur de la recherche en informatique ou en cyber-sécurité.

Sa première priorité est d'améliorer la résilience des organisations nationales et de piloter **une revue stratégique multi-échelle** du dispositif de l'Etat en matière de cyberrésilience.

Le COCyR mettra également en place un observatoire du risque cyber.

❑ Impact attendu

- Disposer d'une haute autorité en matière de cyber résilience pour guider les évolutions de la stratégie de l'Etat dans ce domaine et faciliter sa mise en œuvre.
- Redéfinir, sur la base des résultats de la revue stratégique, la politique, l'organisation et l'engagement de moyens de l'Etat en matière de cyber résilience

❑ Conditions de réussite

- Implication de hauts responsables des secteurs publics et privés

❑ Ressources à mobiliser

- Mise en place d'un secrétariat permanent doté d'une dizaine d'agents.
- Coût : # 1M€/an

❑ Services en charge de la mise en œuvre

Premier ministre (porteur), ministères de l'économie, de l'intérieur et secrétariat d'Etat chargé du numérique

Action 2 : mettre en place des comités d'analyse et de partage de l'information en cybersécurité (CAPIC)

❑ Objectifs et modalités

Les comités d'analyse et de partage de l'information en cybersécurité (CAPIC) sont destinés à encourager et à faciliter les échanges d'informations en matière de cybersécurité entre leurs membres intervenant dans une même filière industrielle.

Les filières prioritaires sont l'énergie, les finances, les transports, la santé. Le modèle des CAPIC peut être adapté aux besoins des collectivités territoriales.

Ils pourraient être chargés de mettre en place des plateformes dédiées à des usages de sécurité et des expérimentations de solutions innovantes intégrant la dimension « privacy by design » et de mener les études d'impact liées au RGPD.

Les CAPIC pourraient être expérimentés sur une ou deux filières pendant 18 mois avant généralisation. L'aéronautique, (autour d'Airbus) et le secteur de l'énergie pourraient constituer les filières pilotes.

❑ Impact attendu

- Les bénéfices attendus de la mise en place des CAPIC sont ceux du partage d'informations et de la mutualisation.

❑ Conditions de réussite

- Convaincre les filières et les réseaux concernés des avantages d'une telle formule.

❑ Ressources à mobiliser

2 ETP pour assurer l'animation et le secrétariat des CAPIC. Les travaux seront assurés par les professionnels du secteur, en particulier l'expérimentation de solutions et la remontée d'informations.

❑ Services en charge de la mise en œuvre

DGE (porteur) , ANSSI, Comités de filières, COFIS, ministères de « tutelle » des filières, Régions de France, Association des maires de France.

Renforcer la gouvernance interministérielle en matière de cyber résilience

Mesurer le niveau de maturité de cyber résilience des organisations, structurer la remontée d'information

Améliorer la cyber résilience des organismes publics

Disposer de compétences nécessaires en cybersécurité

Faciliter l'émergence de produits et solutions innovants en matière de cybersécurité

Mettre le numérique au service de la résilience

Réglementer et réguler pour réduire les risques

Aller au sommaire

Agir contre la sous déclaration des attaques

Une connaissance aussi précise que possible du risque cyber et de ses implications en termes économiques, humains et structurels est un préalable à toute action de prévention ou de réparation efficace. Les Pouvoirs publics en France et en Europe ont bien pris conscience de cet état de fait et de nombreuses mesures ont été mises en œuvre pour une meilleure identification du risque cyber et de ses conséquences, notamment par la mise en place d'obligations déclaratives des incidents cyber pour certains secteurs d'activité ou la mise à disposition de plateformes de signalement volontaire des incidents ouvertes à tous les acteurs économiques. Pour autant, l'efficience globale de ces dispositifs reste encore à évaluer.

Les obligations déclaratives des opérateurs d'importance vitale

L'article L1332-1 code de la défense dispose que « les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, sont tenus de coopérer à leurs frais dans les conditions bien définies, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative ». Au titre de ce principe de coopération, l'article L1332-6-2 du code de la défense précise que les opérateurs informent sans délai le Premier ministre des incidents affectant le fonctionnement ou la sécurité des systèmes d'information pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou pourrait présenter un danger grave pour la population.

En application de ces dispositions, le décret n°2015-351 du 27 mars 2015 a introduit dans le code de la défense l'article R1332-41-10 qui prévoit que « les opérateurs d'importance vitale communiquent à l'Agence nationale de la sécurité des systèmes d'information les informations relatives aux incidents affectant la sécurité ou le fonctionnement de leurs systèmes d'information d'importance vitale. Les opérateurs communiquent les informations dont ils disposent dès qu'ils ont connaissance d'un incident et les complètent au fur et à mesure de leur analyse de l'incident. Ils répondent aux demandes d'informations complémentaires de l'Agence nationale de la sécurité des systèmes d'information concernant l'incident ».

A la suite, plusieurs arrêtés sectoriels sont venus préciser les informations qui doivent être communiquées, les modalités de leur transmission ainsi que les types d'incident auxquels s'applique l'obligation. A ce jour, les secteurs traités sont les produits de santé, la gestion de l'eau, les transports terrestre, maritime, fluvial et aérien, l'approvisionnement en énergie électrique, en gaz naturel et en hydrocarbures pétroliers, l'industrie, les communications électroniques et internet, les finances, l'audiovisuel et l'information, le nucléaire, les activités industrielles de l'armement et de l'espace.

Tout opérateur relevant du secteur concerné déclare chaque incident qui relève d'un type figurant à l'annexe IV de l'arrêté (non publiée) en adressant à l'Agence nationale de la sécurité des systèmes d'information le formulaire de déclaration disponible sur le site internet de l'agence (www.ssi.gouv.fr) selon le moyen approprié à la sensibilité des informations déclarées. Le formulaire est un document confidentiel susceptible de contenir des informations dont la révélation est réprimée par les dispositions de l'article 226-13 du code pénal. Il est, le cas échéant, couvert par le secret de la défense nationale.

Le formulaire de déclaration indique que « les informations anonymisées pourront notamment être partagées par l'ANSSI avec les OIV du même secteur afin de renforcer leur capacité à détecter des attaques sophistiquées ».

D'autres obligations déclaratives sectorielles complémentaires existent

Pour le secteur des communications électroniques :

Dans le cadre de la transposition de la directive 2009/140 du 25 novembre 2009, il a été inséré à l'article D98-5 du code des postes et des communications électroniques les dispositions suivantes : « dès qu'il en a connaissance, l'opérateur informe le ministre de l'intérieur de toute atteinte à la sécurité ou perte d'intégrité ayant un impact significatif sur le fonctionnement de ses réseaux ou de ses services. Ce dernier en informe le ministre chargé des communications électroniques ainsi que les services de secours et de sécurité susceptibles d'être concernés. Lorsque l'atteinte à la sécurité ou la perte d'intégrité résulte ou est susceptible de résulter d'une agression informatique, l'opérateur en informe également l'autorité nationale de défense des systèmes d'information ».

Dès que l'opérateur a mené une analyse des causes et des conséquences des atteintes à la sécurité ou pertes d'intégrité, il doit rendre compte des mesures prises pour éviter leur renouvellement.

Les administrations veillent à la confidentialité des informations qui leur sont communiquées. Toutefois, lorsqu'il est d'utilité publique de divulguer les faits, le ministre de l'intérieur peut en informer le public ou demander à l'opérateur en cause de le faire.

Lorsque l'atteinte à la sécurité ou la perte d'intégrité est susceptible d'avoir un impact significatif dans un ou plusieurs des Etats membres de l'Union européenne, le ministre chargé des communications électroniques, en liaison avec l'ANSSI, informe les autorités compétentes des Etats membres et l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) des atteintes survenues.

Pour le secteur de la santé :

Depuis la loi du 2 janvier 2016, le code de la santé publique contient un article L1111-8-2 disposant que « *les établissements de santé et les organismes et services exerçant des activités de prévention, de diagnostic ou de soins signalent sans délai à l'agence régionale de santé les incidents graves de sécurité des systèmes d'information. Les incidents de sécurité jugés significatifs sont, en outre, transmis sans délai par l'agence régionale de santé aux autorités compétentes de l'Etat* ». Ces dispositions ont été précisées par le décret n°2016-1214 du 12 septembre 2016 qui indique que la déclaration des incidents graves de sécurité des systèmes d'information est destinée à fournir aux autorités compétentes de l'Etat les informations nécessaires pour décider des mesures de prévention en matière de sécurité des systèmes d'information et à aider les établissements de santé, organismes et services exerçant des activités de prévention, de diagnostic ou de soins à prendre toute mesure utile pour prévenir la survenue ou limiter les effets d'incidents graves de sécurité des systèmes d'information, c'est-à-dire ceux qui peuvent provoquer une situation exceptionnelle, notamment les incidents ayant des conséquences potentielles ou avérées sur la sécurité des soins ou sur la confidentialité et l'intégrité des données de santé et ceux portant atteinte au fonctionnement normal de l'établissement.

Pour le secteur de la banque :

Depuis l'été 2017, les banques victimes de cyberattaques, ou de tentatives de cyberattaques, doivent les déclarer à la Banque centrale européenne (BCE). Cette obligation de déclaration porte sur les incidents informatiques significatifs et s'applique aux 130 banques supervisées directement par la BCE, les enseignes dites systémiques, dont le bilan dépasse les 30 milliards d'euros. En France, 7 grandes enseignes, représentant 90% du marché, sont concernées : BNP Paribas, BPCE, Crédit Agricole SA, Société Générale, Confédération nationale du Crédit Mutuel, HSBC France et la Banque Postale.

Aller au sommaire

Malgré ces obligations, il apparaît que l'appréciation du niveau réel de risque, de l'état de préparation des organisations publiques et privées et la mesure des conséquences directes sur l'économie et la sécurité des français restent perfectibles.

Sans méconnaître la nécessité de préserver la confidentialité de certaines informations, la publication d'un rapport annuel de l'ANSSI, à partir de l'ensemble des informations qu'il collecte, anonymisé, permettrait une juste appréciation collective de l'état de la menace et de ses conséquences .

La nécessité de référentiels

Il n'existe pas au niveau français ou européen, de référentiel communément accepté pour évaluer le niveau de maturité de cyber résilience des organisations.

L'un des éléments clés de la sécurité qui manque dans les guides européens, mais qui figure dans le programme des États-Unis, est l'utilisation d'une approche fondée sur les risques. Dans les programmes européens, il y a peu ou pas d'indications pour les entreprises en ce qui concerne l'évaluation de leurs risques individuels, l'identification des actifs à haut risque et la mise à l'échelle de leur sécurité pour implémenter une approche de type "joyaux de la couronne"
(ENISA, 12/2016)

Compte tenu de la numérisation croissante des services financiers et de l'évolution du paysage des cybermenaces, il est important de poursuivre des approches efficaces pour l'évaluation de la cybersécurité au niveau des entreprises financières et du secteur dans son ensemble (...)
Très conscients de la pertinence transfrontalière et intersectorielle des cybermenaces, nous chargeons le G7 GCE de faire avancer les travaux sur les risques liés aux tiers et la coordination avec d'autres secteurs critiques.
Communiqué G7 Finance Ministers and Central Banks' Governors Meeting 5/2017

La FERMA (Fédération des Associations Européennes de Gestion des Risques) estime qu'une intervention publique est nécessaire, notamment dans les domaines énumérés ci-dessous afin de soutenir les organisations et notamment les risk managers dont le rôle est d'identifier, quantifier, évaluer, atténuer et transférer les risques:
- Établir un cadre commun de responsabilité tout au long de la chaîne d'approvisionnement pour les clients finaux. Ce cadre commun définirait clairement qui porte quel risque et dans quelle proportion.
- Développer un cadre pour l'évaluation des risques de cybersécurité, notamment en incluant un processus de certification conforme pour les organisations et une divulgation obligatoire aux autorités publiques de l'exposition aux risques.

Au niveau international , on note la publication par le US Departement of Homeland Security d'un référentiel relativement complet d'évaluation de la cyber résilience des organisations (cf. annexe N°6)
(https://www.us-cert.gov/ccubedvp/assessments)

Dans l'attente d'une mobilisation européenne, il nous apparaît que les acteurs français doivent se mobiliser pour établir ce référentiel. De façon plus précise, il est nécessaire d'établir quatre référentiels, adaptés à quatre catégories d'organisations :

- Les grandes entreprises et ETI
- Les TPE, PME et associations
- Les collectivité territoriales et opérateurs de l'Etat non couverts par la PSSI
- Les entités publiques assujetties à la PPSIE

Tous les *points essentiels* (Cf. supra) doivent être traités dans ces référentiels qui permettront d'établir **un niveau synthétique de cyber résilience (NSCR)** .

Ces référentiels doivent être élaborés avec le concours de l'ensemble des acteurs concernés (ANSSI, assureurs, organisations patronales, CIGREF, commissaires aux comptes, organisations sectorielles, auditeurs).

Concernant l'Etat, une actualisation de la PSSIE (cf. recommandation N° 3) devra intégrer ce référentiel d'évaluation de la cyber résilience . On notera, à ce propos, les travaux de l'Etat australien qui communique largement sur la méthode et les résultats de l'audit de ses structures gouvernementales :

https://www.asd.gov.au/infosec/ism/index.htm

https://www.anao.gov.au/work/performance-audit/cybersecurity-follow-audit

Mesurer la réalité du risque cyber et de ses conséquences et dépasser une démarche encore trop techno centrée

L'identification, la quantification et l'évaluation des risques cyber et surtout de leurs impacts font aujourd'hui défaut que ce soit pour les entreprises, les administrations, les particuliers alors qu'à peu près tous ces risques augmentent rapidement dans des proportions qui paraissent importantes.

Le dispositif ACYMA (https://www.cybermalveillance.gouv.fr/), mis en place par l'ANSSI et déployé fin 2016 au plan national, vise en premier lieu à mettre en relation les victimes de cyber attaque, entreprises ou particuliers, avec des professionnels susceptibles de les accompagner. Il constitue également un moyen d'évaluer la réalité du risque cyber, son évolution et ses conséquences propre à alimenter l'observatoire de la cybersécurité (cf. recommandation 1)

➡ Mettre en ligne un formulaire de déclaration volontaire des incidents cyber sur le site www.cybermalveillance.gouv.fr inspiré de celui mis à disposition des OIV. Ce formulaire devrait inclure une rubrique sur les conséquences financières estimées des incidents cyber.

➡ Prévoir à partir de la fin 2018 une évaluation du dispositif mis en place dans le cadre du GIP-ACYMA pour en ajuster au besoin les modalités.

Sur la dimension économique toujours, il est regrettable de ne pas pouvoir disposer d'une évaluation fiable de la fréquence et des conséquences financières des incidents cyber. Les études disponibles, le plus souvent commanditées et financées par des offreurs de solutions de cybersécurité, n'offrent aucune garantie d'indépendance. Elles sont par ailleurs très discutables du point de vue méthodologique. Les échantillons sont souvent réduits, les résultats publiés de façon parcellaire et aucun accès exhaustif aux données détaillées n'est proposé.

La dernière étude de l'INSEE publiée sur le thème en 2016 s'appuie sur des données recueillies en 2014, donc déjà anciennes, compte tenu de la rapide évolution du phénomène des cyber attaques. Par ailleurs, elle n'apporte pas d'information sur les conséquences économiques de ces attaques. Les données statistiques disponibles sur le site de Eurostat présentent les mêmes limites.

➡ La mise en œuvre d'une étude statistique officielle sur ce thème serait de nature à éclairer un phénomène dont l'impact réel en France reste mal connu et sujet à interprétation. Cette étude pourrait être confiée à l'INSEE. Il est souhaitable d'associer les acteurs publics et privés intéressés à la définition du cahier des charges de l'étude..

Plus globalement, il est proposé que le conseil d'orientation de la cyber résilience (Cf. Recommandation N°1) mette en place un observatoire interministériel des risques de cybersécurité et de leurs conséquences.

Recommandation N° 2 - Mesurer le niveau de maturité de cyber-résilience des organisation, structurer la remontée d'information

❑ Objectifs et modalités

- **Action 1 : constituer un référentiel d'évaluation de la cyber résilience des organisations avec quatre déclinaisons pour :**
  - **Les grandes entreprises et ETI**
  - **Les TPE, PME, et associations.**
  - **Les collectivités et organismes publics, non couverts par la PSSI de l'Etat**
  - **Les entités publiques assujetties à la PSSIE (Cf. recommandation N°3)**

Ces référentiels doivent permettre à chaque organisation de réaliser (ou faire réaliser) une revue de cyber résilience conduisant à l'estimation du **NSCR** (N**iveau Synthétique de Cyber Résilience**)

La mise en œuvre des revues doit se faire en priorité pour les organisations les plus sensibles aux risques numériques.

- **Action 2 : organiser, sur la base des remontées d'incidents enregistrées par l'ANSSI et les autres sources d'information sectorielle, la préparation d'un rapport annuel anonymisé destiné à une large diffusion permettant d'évaluer l'évolution du risque cyber et de caractériser au mieux les incidents**

❑ Impact attendu

- Objectivation et renforcement des audits de cyber résilience sur la base d'un référentiel partagé et reconnu et d'indicateurs labellisés
- Emergence d'une mesure de la cyber résilience facilitant l'assurabilité de ce type de risques
- Le NSCR est un repère simple et synthétique de la situation de chaque organisation pour décider de se priorités opérationnelles
- Meilleure connaissance de l'évolution des risques, des parades et des conséquences économiques des attaques.

❑ Conditions de réussite

- Association de l'ensemble des parties prenantes (ANSSI, DGE, entreprises de cyber sécurité, auditeurs , assureurs, AMF pour les sociétés cotées, fédérations professionnelles, les collectivités locales…) à l'élaboration des référentiels et à la mise en place de l'observatoire.
- Adaptation de la complexité de chaque référentiel à la cible visée
- Utilisation des modèles existant comme point de départ (CRR du CERT-US en particulier Cf. annexe 7)
- Dispositif de portage du référentiel et de son actualisation intégré dès le départ.

❑ Ressources à mobiliser

- Quatre groupes de travail pour 6 mois environ pour les référentiels
- Publication et diffusion du référentiel

❑ Services en charge de la mise en œuvre

ANSSI (porteur), DGE, CHAI, parties prenantes

Renforcer la gouvernance interministérielle en matière de cyber résilience

Mesurer le niveau de maturité de cyber résilience des organisations, structurer la remontée d'information

Améliorer la cyber résilience des organismes publics

Disposer de compétences nécessaires en cybersécurité

Faciliter l'émergence de produits et solutions innovants en matière de cybersécurité

Mettre le numérique au service de la résilience

Réglementer et réguler pour réduire les risques

Aller au sommaire

Améliorer la cyber résilience des organismes publics

Un seul indicateur permet d'identifier le niveau de sécurité des SI de l'Etat. Il concerne l'OBJECTIF 6 de la LOLF : *La sécurité et la performance des systèmes d'information de l'Etat*.

Il s'agit de l'indicateur de maturité globale en sécurité des SI de l'Etat présenté annuellement lors des débats sur la loi de finance

Niveau de sécurité des systèmes d'information de l'Etat

(du point de vue de l'usager)

Source RAP 2016	Unité	2014 Réalisation	2015 Réalisation	2016 Prévision PAP 2016	2016 Prévision actualisée PAP 2017	2016 Réalisation	2017 Cible PAP 2016
Maturité globale en sécurité des systèmes d'information de l'Etat	note de 0 à 5	3,3	2,3	2,4	2,6	2,5	2,7

La moitié des FSSI note l'insuffisance de ressources financières et humaines dans leurs ministères, l'évolution de la menace, l'ouverture des systèmes d'information (utilisateurs extérieurs à l'administration, nomadisme, …) et le fait que le critère de la sécurité passe généralement loin derrière ceux des coûts et de la facilité d'usage dans les investissements ou dans l'affectation de ressources humaines.'' - PAP 2015

''Le niveau de sécurité moyen atteint a ce jour reste toutefois insuffisant au regard des enjeux portes par les systèmes d'information de l'Etat.''
– RAP 2016

L'indicateur de maturité globale en sécurité des SI de l'Etat fait apparaitre le besoin d'une relance de la mobilisation des ministères en matière de cybersécurité. Le renouvellement de la PSSIE et de son accompagnement parait opportun.

Face à l'augmentation des risques, la définition d'une politique de cyber -résilience pour chaque ministère est par ailleurs souhaitable, la démarche nationale du SGDSN dans ce domaine étant limitée à un nombre restreint d'acteurs.

Il est d'autre part nécessaire que les risques sémantiques (influence, désinformation ou manipulation de l'information) soient mieux connus par l'encadrement des ministères.

Aller au sommaire

Recommandation n° 3 - Améliorer la cyber résilience des organismes publics (1/2)

❑ Objectifs et modalités

- **Action 1 : Renouveler la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) établie en 2014 afin de :**

  - **Procéder à la mise à jour des éléments techniques et organisationnels qu'elle doit comporter**. Cela concerne notamment :
    - Un meilleur cadrage des questions relatives au Cloud, au télétravail, au recours aux outils nomades ou de type BYOD.
    - La prise en compte des objets connectés.

  - **Renforcer l'implication générale des personnels de l'administration en matière de cybersécurité**, à savoir :
    - Une implication du personnel des ministères qui doit participer à son niveau à la sécurité du SI.
    - Une implication de l'encadrement des ministères avec, le cas échéant, des répartitions de rôles et de responsabilités spécifiques parmi la hiérarchie des directions métier.
    - Cette implication doit pouvoir être accompagnée par des règles formelles qui peuvent, le cas échéant, être contraignantes.

  - **Doter la PSSIE d'instruments destinés à soutenir et accompagner sa mise en œuvre au profit des personnels qu'elle concerne**.
    - Par la mise en place d'un dispositif de soutien et d'accompagnement à sa mise en œuvre au profit des responsables ministériels de la sécurité des SI ainsi que du personnel administratif : éléments de communication, MOOC, automatisation du reporting quand c'est possible,…

  - **Inclure une dimension de résilience rendue nécessaire par l'accroissement des risques et l'augmentation de la probabilité de leur occurrence**.
    - En définissant une politique de cyber-résilience destinée notamment à évaluer ce qui doit être impérativement protégé au sein de la structure en fonction des trois critères stratégiques : disponibilité, intégrité, confidentialité.
    - En améliorant la planification des réactions en cas d'attaque par un renforcement des plans de continuité de l'activité (PCA) ou de reprise de l'activité (PRA) accompagné d'une méthodologie et d'outils destinés à faciliter leur définition et leur mise en œuvre. Ces plans devront être testés régulièrement. Cette planification doit inclure un plan de gestion de crise qui doit prévoir la participation de certaines directions de soutien des ministères (RH, COM interne,…)
    - En invitant à la mise en œuvre annuelle d'un **référentiel d'évaluation de la cyber-résilience (Cf. RECO 2)**

❑ Impact attendu

- Renforcement de la cyber-résilience

❑ Conditions de réussite

- Prise en compte des différents contextes ministériels

❑ Ressources à mobiliser

- FSSI, RSSI, RH des ministères

❑ Services en charge de la mise en œuvre

ANSSI (porteur) , CHAI, SG des ministères

Recommandation n° 3 - Améliorer la cyber résilience des organismes publics (2/2)

- **Action 2 : Auditer les ministères, organismes publics et collectivités locales, sur la base des référentiels d'évaluation de la cyber-résilience.**
- **Objectifs et modalités**
  - Ces évaluations devront dans un premier temps être conduites par des agents extérieurs au ministère concerné. Elles pourront par la suite être conduites par les HFDS.
  - Elles devront également porter sur le niveau de la « dette technique » et son impact sur la résilience.

❑ **Conditions de réussite**

- Définition préalable d'un référentiel d'évaluation de la cyber-résilience.

❑ **Ressources à mobiliser**

- Equipes d'auditeurs internes et externes.
- Coût # 200 K€/ministère

❑ **Services en charge de la mise en œuvre**

ANSSI (porteur), CHAI, SG, HFDS

❑ **Impact attendu**

- Amélioration de la cyber-résilience de la structure.

- **Action 3 : Former et mobiliser décideurs, managers et ingénieurs sur le risque cyber, en particulier sémantique (manipulation, réputation, démocratie).**

❑ **Conditions de réussite**

- Définition d'un programme de formation adapté.

❑ **Ressources à mobiliser**

- Experts publics et privés.

❑ **Services en charge de la mise en œuvre**

ANSSI (porteur), SG des ministères , DGAFP

❑ **Impact attendu**

- Améliorer la gestion de ce type de risque.

- Renforcer la gouvernance interministérielle en matière de cyber résilience
- Mesurer le niveau de maturité de cyber résilience des organisations, structurer la remontée d'information
- Améliorer la cyber résilience des organismes publics
- **Disposer de compétences nécessaires en cybersécurité**
- Faciliter l'émergence de produits et solutions innovants en matière de cybersécurité
- Mettre le numérique au service de la résilience
- Réglementer et réguler pour réduire les risques

Aller au sommaire

❑ Augmenter le flux de formation, maintenir les compétences sur la durée, fidéliser nos talents sur nos enjeux

Le dispositif de formation national en matière de cybersécurité est d'une haute qualité mais peine à fournir le flux nécessaire aux besoins des secteurs public et privé.

La cyber-sécurité est un sujet de formation depuis de nombreuses années. Des programmes solides existent et font référence dans ce domaine. Ainsi, la formation ESSI de l'ANSSI existe depuis une vingtaine d'années, même si elle a subi de nombreuses transformations durant cette période. La spécialisation en Sécurité des Systèmes et des Réseaux de Télécom Sud Paris existe depuis plus de 12 ans, dans sa version intégrée au programme ingénieur et sous forme de Mastère Spécialisé. Un vivier significatif d'étudiants a donc pu être formé ces dernières années.

Les différents mécanismes de labellisation et de coopération avec l'ANSSI permettent de valider à la fois la pertinence et la qualité des formations. Le programme CyberEdu fournit à toute formation aux domaines du numérique des outils pour intégrer la cyber-sécurité dans le programme de formation. La labellisation SecNumedu valide pour les étudiants et les entreprises le fait qu'une formation, au niveau M2, est conforme au référentiel de compétences et de métiers cyber-sécurité.

Le bon fonctionnement d'une formation repose également sur une équipe de recherche solide, dont l'activité permet d'assurer une bonne visibilité à la formation. Cela permet d'organiser des stages, dont certains à l'étranger, d'obtenir des sujets de projets, et de maintenir un vivier de vacataires professionnels du domaine de la cyber-sécurité pour animer les formations.

Pour accroitre suffisamment le flux de formation, il s'agit donc de promouvoir la cyber-sécurité au sein des pôles d'excellence, développer des plateformes d'apprentissage et d'expérimentation, accroître le vivier d'étudiants susceptibles de suivre des formations en cyber-sécurité et de devenir des professionnels du domaine, développer des mécanismes de certification des compétences.

Maintenir les compétences dans la durée par un dispositif de formation constitue un objectif indispensable alors que l'évolution des technologies, l'innovation qu'elles permettent, le renouvellement et l'intensification des menaces imposent des remises à jour très régulière des connaissances des experts du domaine. Pour l'heure, un tel dispositif n'existe pas et doit être conçu ex-nihilo.

La fidélisation des compétences doit également faire l'objet d'un effort particulier. La France possède une expertise reconnue notamment dans les filières cryptologie, algorithmique, méthodes formelles et forme des experts très recherchés au niveau mondial qui ont tendance à s'expatrier.

Aller au sommaire

Recommandation n° 4 - Disposer de compétences nécessaires en cybersécurité (1/2)

- **Action 1 : renforcer la diffusion de la cyber-sécurité dans la formation initiale et continue, développer les formations spécifiques post-bac, en particulier au niveau technicien (UIT, BTS) et ingénieur**

Objectifs et modalités

Il s'agit d'augmenter le flux de formation en particulier pour ce qui concerne les techniciens. Ce projet pourrait être intégré dans le plan d'action du commissaire à la transformation des compétences

Impact attendu

- Disposer d'un flux de formation à la hauteur des besoins des secteurs publics et privé.

Conditions de réussite

- Mobilisation des filières de formation de l'enseignement supérieur.

Ressources à mobiliser

- Le cas échéant, subventions destinées à l'amorçage des formations concernées.

Services en charge de la mise en œuvre

DGESIP (porteur) , ANSSI, IMT, DGE, Haut commissaire à la transformation des compétences

- **Action 2 : Mettre en place un dispositif de formation continue et de fidélisation associé à un label.**

Objectifs et modalités

Le projet pourrait s'appuyer sur une association de centres de formation initiale pour développer une offre de formation continue mutualisée et répartie entre les différents centres. Il s'agit de faire en sorte que la ''formation tout au long de la vie'' soit proposée dans tous les domaines spécialisés de la cybersécurité. Un label spécifique serait décerné à ces formations continues.

Un autre label serait proposé aux professionnels qui suivraient ces formations avec le niveau de régularité requis pour garantir une mise à jour de leurs compétences répondant aux besoins du domaine. Ce label permettrait la constitution d'un réseau d'experts qui disposerait d'une animation spécifique et de certains services utiles à ses membres (services RH, outplacement,…).

Le financement du dispositif de formation continue pourrait être pris en charge par les OPCA et l'Etat. Celui de l'animation et des services du réseau des experts labelisés pourrait être réparti entre l'Etat et les partenaires du COFIS concernés par la cybersécurité.

Impact attendu

- Fidélisation d'un nombre d'experts suffisants pour les besoins prioritaires de l'Etat et des OIV.

Conditions de réussite

- Mobilisation de certains centres de formation de l'enseignement supérieur. Création d'un cycle de formation continue intégré.

Ressources à mobiliser

- Spécialistes de la formation en cybersécurité pour concevoir programmes et parcours de formation

Services en charge de la mise en œuvre ou en appui

ANSSI, ministères des armées, de l'intérieur, de l'enseignement supérieur, IMT

Recommandation n° 4 - Disposer de compétences nécessaires en cybersécurité (2/2)

- **Action 3 : Mettre en place une GPEEC des spécialistes en cyber-sécurité au sein de la sphère publique en valorisant les parcours public-privé**

❑ Objectifs et modalités

Identifier les compétences en cyber sécurité nécessaires au sein de chaque service, puis évaluer les potentiels en place. Garantir une gestion prévisionnelle des emplois, des effectifs et des compétences en liaison avec les organismes de formation en privilégiant les postes les plus sensibles.

❑ Impact attendu

Disponibilité des compétences nécessaires pour mettre en œuvre la PSSIE au sein de la sphère publique et garantir un niveau correct de résilience des SI.

❑ Conditions de réussite

Implication de la DGAFP et de l'ANSSI pour accompagner les ministères dans la mise en œuvre d'une GPEEC adaptée aux besoins spécifiques de la cyber sécurité.

❑ Ressources à mobiliser

Les DRH des services des ministères pour la mise en oeuvre, la DGAFP pour coordonner et accompagner les ministères

❑ Services en charge de la mise en œuvre ou en appui

DGAFP (porteur) , ministères (DRH), DSAF, ANSSI, IMT

- **Action 4 : Maîtriser la politique d'externalisation des ministères, en particulier dans les fonctions liées à la cybersécurité**

❑ Objectifs et modalités

Les ministères qui ont externalisé à l'excès leur cybersécurité risquent de voir leur capacité de réaction pénalisée en cas d'attaque majeure, et cela concerne aussi les OIV. Pour maîtriser la capacité de protection des systèmes, il est nécessaire d'avoir des équipes de confiance souveraines ou pas, d'opérer en interne les systèmes afin d'être en mesure de les réparer le cas échéant, et pour cela définir le socle indispensable de compétences à conserver en interne, puis élaborer une stratégie de sous-traitance non subie .

❑ Impact attendu

Disposer des compétences internes nécessaires pour garantir l'appropriation de la cybersécurité par la structure ainsi que sa capacité à réagir de manière autonome et sans délai en cas d'agression. Garantir sur le plan « cyber » la résilience des métiers.

❑ Conditions de réussite

Compétence de la maîtrise d'ouvrage au sein des directions métier

❑ Ressources à mobiliser

Des directeurs de projets formés et mobilisés au sein des directions métiers et une participation active des directeurs des système d'information.

❑ Services en charge de la mise en œuvre

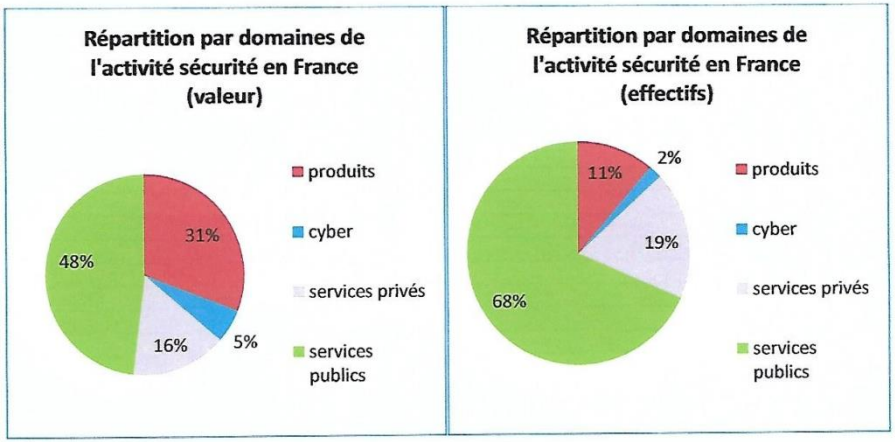
ANSSI, DINSIC (porteur) , IMT, ministères (SG, DSI)

- Renforcer la gouvernance interministérielle en matière de cyber résilience
- Mesurer le niveau de maturité de cyber résilience des organisations, structurer la remontée d'information
- Améliorer la cyber résilience des organismes publics
- Disposer de compétences nécessaires en cybersécurité
- **Faciliter l'émergence de produits et solutions innovants en matière de cybersécurité**
- Mettre le numérique au service de la résilience
- Réglementer et réguler pour réduire les risques

Aller au sommaire

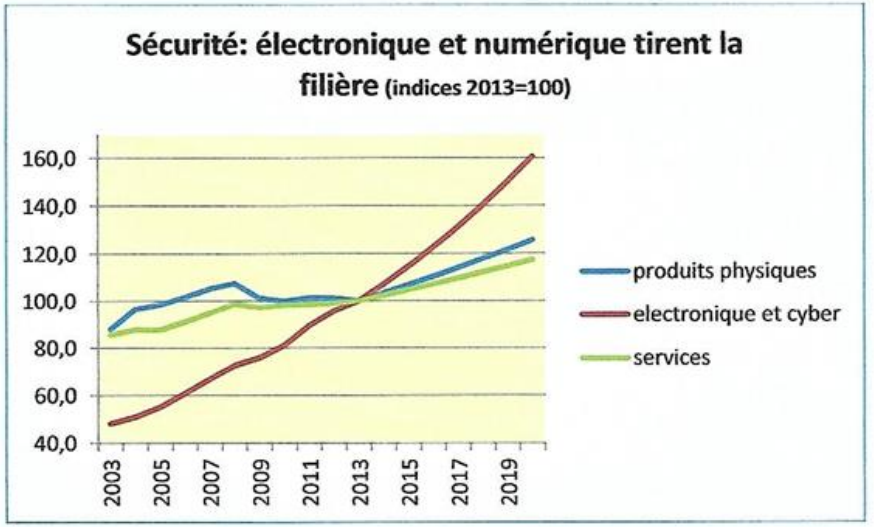
Le comité de la filière industrielle de la sécurité (CoFIS)

Institué en 2013, le comité de la filière industrielle de sécurité (CoFIS) a pour objectif de mettre en réseau les compétences publiques et privées, afin de répondre aux objectifs de la filière tout en responsabilisant l'ensemble des parties prenantes. Sa composition et son mode de fonctionnement associent les intervenants pertinents du domaine. **Cependant, la dimension cyber est très diluée dans la filière sécurité alors qu'elle en constitue le principal moteur de croissance .**



Répartition du chiffre d'affaires brut et des emplois de la sécurité en France en 2013 sur le secteur marchand

Segment		CA France Md€	Emplois
Industrie et services associés	Produits physiques	5,33	35 300
	Produits électroniques	12,43	71 500
	Cybersécurité	3,14	18 500
	Total	**20,90**	**125 300**
Services de sécurité privée		9,00	176 900
TOTAL SECTEUR MARCHAND		**29,90**	**302 200**



Faciliter l'émergence de produits et solutions innovants en matière de cybersécurité

C'est en substance ce que défendent **Marc Darmon, président du conseil des industries de la confiance et de la sécurité (CICS)**

« Une action volontariste doit être menée à plusieurs niveaux : soutien à l'innovation, investissements, défense de la base industrielle et de souveraineté, soutien à l'exportation, gouvernance étatique de la sécurité, coopération européenne. En matière de soutien à l'innovation, le CICS estime que l'Etat doit se fixer pour but d'investir un milliard sur trois ans dans l'innovation technologique pour résister à la forte concurrence mondiale et placer la France à l'avant-garde des ruptures technologiques et de marchés. Il s'agit de s'aligner sur les pays qui investissent massivement sur les technologies de sécurité pour ne pas risquer le déclassement et la dépendance.
Nous souhaitons élever l'efficacité de la sécurité et la résilience du pays par une gouvernance claire et unifiée au niveau de l'Etat. Le dialogue inauguré depuis 2013 au sein du COFIS (comité de la filière des industries de sécurité), présidé par le Premier ministre, entre les pouvoirs publics, les industriels et leurs partenaires du domaine de la recherche constitue une avancée importante pour défragmenter le domaine de la sécurité. Il faut aller plus loin ***et se donner les moyens d'un pilotage global et transverse avec une impulsion à donner à la politique publique de sécurité, aux budgets de recherche et aux programmes d'équipement. »***

Marc Darmon*, (tribune publiée dans le journal Les Echos le 24 août 2017) :*

… et Stéphane Schmoll, conseiller de Deveryware et Président de la commission stratégique du CICS

« On pourrait mettre enfin en cohérence la future politique industrielle du COFIS, les feuilles de route des pôles de compétitivité et les guichets nationaux ANR, FUI, RAPID, PIA … à leurs tranches de TRL ***respectives en mutualisant les multiples comités d'analyse, d'expertise et de décision dans une autorité commune*** *(…), on pourra encore optimiser le test, le déploiement opérationnel, la certification et peut-être même la commercialisation des solutions. Les projets de plateformes peuvent y apporter des réponses séduisantes (…) Mais pratiquement aucune n'a jusqu'à présent été consacrée à des solutions de sécurité, alors que le concept avait été proposé dès 2010 dans les travaux menés sous l'égide du SGDSN consacrés à des feuilles de route technologiques nationales qui ont préfiguré la création de la filière (…). Il serait donc judicieux de mettre en place des plateformes dédiées à des usages de sécurité, qui soient capables de parangonner différents composants, sous-systèmes ou systèmes dans des environnements proches de la réalité et de ses divers cas d'usage et contraintes. Cela fournirait des référentiels objectifs de test, de validation voire de certification (…). Cela favoriserait aussi la mutualisation des solutions, donc l'efficience, au sein des utilisateurs publics et privés, ainsi que l'exportation de nos entreprises en s'appuyant sur des vitrines nationales. Il serait bon de concentrer sur ces plateformes d'évaluation opérationnelle et de certification (PEOCE) l'expérimentation de solutions audacieuses cherchant à apporter les garanties nécessaires en combinant « privacy by design » et études d'impact conformément au règlement général européen pour la protection des données.*
Notre pays possède tous les atouts nécessaires pour accélérer les débouchés de sa filière industrielle de sécurité tout en maximalisant l'efficience et la confiance, avec une mobilisation accrue de acteurs du COFIS et du CICS. »

Stéphane Schmoll *(Revue S&D, sécurité et défense Mai 2017)*

Aller au sommaire

Recommandation n° 5 - Faciliter l'émergence de produits et solutions innovants en matière de cybersécurité

❑ Objectifs et modalités

➢ **Mettre en place des outils tels que des plateformes dédiées à des usages de sécurité, pour développer des offres nationales intégrées associant le monde de la recherche, les grands groupes, les intégrateurs et les fournisseurs de solutions**

➢ **Concentrer sur ces plateformes l'expérimentation de solutions innovantes intégrant la dimension « privacy by design » et les études d'impact liées au RGPD afin de développer des offres de solutions françaises exportables qui intègrent les obligations de ce règlement**

➢ **Mutualiser les comités d'analyse, d'expertise et de décision pour l'attribution des aides publiques dans le domaine de la cybersécurité (ANR, FUI, RAPID).**

❑ Impact attendu

- Renforcement de l'offre française de solutions en matière de cybersécurité en France et à l'export ;
- Meilleure réactivité de la filière aux évolutions réglementaires et technologiques.

❑ Conditions de réussite

- S'appuyer sur le conseil des industries de la confiance et de la sécurité (CICS) qui regroupe les industriels concernés pour la définition des outils ;
- Possibilité de déroger aux lois et règlements en vigueur dans des conditions précises pour développer les expérimentations.
- Porter le « noyau PME français » et les entités qui les fédèrent au niveau européen, en encourageant les rapprochements, en particulier entre la France et l'Allemagne.

❑ Ressources à mobiliser :

- Le Comité stratégique de filière des industries de la sécurité (CoFIS) qui doit orienter davantage son action sur la dimension cyber ;

- Les tutelles du CoFIS (DGE, SGDSN)
- Le Conseil d'orientation de la cyber résilience (Cf. recommandation N°1)

❑ Services en charge de la mise en œuvre

DGE (porteur), SGDSN, IMT, CNIL (aspects RGPD)

Renforcer la gouvernance interministérielle en matière de cyber résilience

Mesurer le niveau de maturité de cyber résilience des organisations, structurer la remontée d'information

Améliorer la cyber résilience des organismes publics

Disposer de compétences nécessaires en cybersécurité

Faciliter l'émergence de produits et solutions innovants en matière de cybersécurité

Mettre le numérique au service de la résilience

Réglementer et réguler pour réduire les risques

Aller au sommaire

❑ Mobiliser les communautés

Dans le domaine de la gestion de crises liées à des catastrophes naturelles ou environnementales, plusieurs organisations ont vu le jour ces dernières années pour intervenir en soutien des secours grâce à des moyens cyber. Il s'agit notamment de Humanitarian OpenStreetMap Team (HOT https://www.hotosm.org/) qui mobilise des contributeurs pour cartographier des régions sinistrées et faciliter ainsi l'intervention des secours comme ce fut le cas après le tremblement de terre au Népal. L'association VISOV (Volontaires Internationaux en Soutien Opérationnel Virtuel http://www.visov.org/) a pour vocation d'aider les secours grâce à l'utilisation des médias sociaux. HAND (Hackers Against Natural Disasters http://hand.team/) s'est fixé pour mission de se préparer à des situations de crise et de mettre à disposition ses compétences dans la phase immédiate post catastrophe. Sa première action a concerné la prévention d'un tsunami dans les Caraïbes. Elle a également été très active suite au passage catastrophique de la tempête IRMA.

❑ Cyber réserve de la Défense Nationale

Il s'agit de pouvoir recourir à un dispositif de réserve activable en cas d'alerte avec un niveau de disponibilité opérationnelle suffisamment élevé pour contrer des attaques massives. Ce principe est à la base de la création du commandement de cyberdéfense, décidée à la fin de 2016, qui devrait disposer, dès 2019, de plus de 4000 réservistes mobilisables pour renforcer un personnel permanent de plus de 2000 militaires spécialisés. Certaines entreprises privées ont annoncé avoir organisé des forces de réserve de spécialistes de cyber sécurité mobilisables dans des conditions équivalentes. Dans les deux cas, les cyber réservistes sont sélectionnés et préparés à la mission qui pourrait les concerner avant que celle-ci soit lancée.

Bonne pratique : l'hypervision du réseau de distribution d'eau « HUBLO » de VEOLIA

Avec son interface de visualisation, basée sur une application cartographique, ainsi qu'avec des outils d'analyses, de génération d'alertes, HUBLO permet à l'exploitant d'optimiser le service (pilotage des installations, interventions, qualité de l'eau, usagers) et à la Métropole de Lyon d'avoir un accès simplifié en un seul visuel consolidant les données principales du service. De plus, en cas de crise, Hublo est également un outil facilitant l'aide à la décision.
C'est une avancée dans le décloisonnement de la donnée métiers, les frontières s'effacent pour plus d'efficacité opérationnelle en toute transparence avec la collectivité.
Cette plateforme a été pensée pour intégrer les logiciels existants et n'oblige pas les collectivités à refaire ce qui est déjà fait. Elle est donc adaptable à toutes situations que ce soit dans des villes très évoluées comme dans des villes où tout est à construire.
Elle a été également pensée pour être évolutive. Elle permet donc le développement de nombreuses fonctionnalités qui peuvent être développées localement, l'intégration de logiciels nouveaux et la mise en valeur immédiate de données de nouveaux capteurs.

Constituer une réserve citoyenne ultra connectée
Le crowdsourcing de la sécurité est un outil de la résilience, par exemple les « hackers bienveillants » qui peuvent être une aide appréciable.
Par ailleurs, suite à un hackathon de trois jours entre la communauté digitale et des spécialistes de la sécurité dans le cadre de l' « école 42 », la ville a prolongé cette dynamique au travers de la plateforme « Nec Mergitur ». Une réserve communale de sauvegarde a été constituée d'une centaine d'agents municipaux en retraite.
En projet : une plateforme internet type OSM (open street map) alimentée par les habitants dans l'objectif d'alerter.
***Sébastien MAIRE**, Haut Responsable de la Résilience de la ville de Paris*

Recommandation n° 6 - Mettre le numérique au service de la résilience

Objectifs et modalités

- **Mobiliser les ressources numériques et les communautés pour accompagner la gestion de crise : communications mobiles, réseaux sociaux (associations RAND, VISOV), voire développer par anticipation des ressources locales autonomes (réseaux électriques locaux, communications satellitaires…)**

- **A l'instar de la Direction générale de sécurité civile et de la gestion des crises (DGSCGC) qui a mis en place un système de conventions avec des associations de proximité telles que VISOV, il s'agit de mobiliser les communautés de volontaires de proximité avec pour objectif de compléter le dispositif de remontée des alertes par la détection d'évènements hors voies traditionnelles.**

Impact attendu

- La mobilisation de forces au niveau local permet d'une part de déployer des moyens supplémentaires de façon très souple et réactive, et d'autre part d'apporter des solutions innovantes et souvent plus adaptées au terrain en cas de crise en s'appuyant sur les capacités du cyberespace (communications satellitaires, réseaux sociaux, …). L'impact serait alors des secours plus rapides et appropriés.

Ressources à mobiliser

- Elaboration d'une stratégie et mise en œuvre par anticipation des conventions par la DGSCGC

Services en charge de la mise en œuvre

- Ministère de l'Intérieur / Protection civile

- Renforcer la gouvernance interministérielle en matière de cyber résilience
- Mesurer le niveau de maturité de cyber résilience des organisations, structurer la remontée d'information
- Améliorer la cyber résilience des organismes publics
- Disposer de compétences nécessaires en cybersécurité
- Faciliter l'émergence de produits et solutions innovants en matière de cybersécurité
- Mettre le numérique au service de la résilience
- Réglementer et réguler pour réduire les risques

Aller au sommaire

❑ Une exception juridique préjudiciable à la sécurité

Comparativement à d'autres secteurs d'activités économiques, l'écosystème du numérique fait figure d'exception tant par sa dynamique propre que par le cadre juridique qui peut le concerner ou dont il s'affranchit. Cette spécificité crée des vulnérabilités grandissantes pour les systèmes et réseaux de tout ordre ainsi que pour leurs utilisateurs exposés à des risques multiformes en augmentation régulière.

La dynamique économique du numérique est fondée sur un couplage d'innovation/obsolescence qui impose aux utilisateurs un renouvellement régulier de leurs équipements, hardware ou software. Deux facteurs principaux y conduisent. D'une part, la nécessité de disposer d'outils performants et compatibles/interopérables., d'autre part , l'obligation faite, au titre de la sécurité, de ne pas utiliser des versions de logiciels anciens dont les éditeurs n'assurent plus la maintenance et qui peuvent présenter des failles de sécurité non corrigées. Il reste que la sécurité d'un produit nouvellement mis sur le marché n'est pas davantage garantie car il faut généralement un certain temps pour que les failles de sécurité les plus évidentes soient traitées si toutefois elles sont détectées.

Le renouvellement régulier des produits aboutit donc mécaniquement à une augmentation sur le même rythme des vulnérabilités non traitées dans l'ensemble des parcs informatiques. Le risque associé touche toutes les catégories d'utilisateurs, que ce soient les particuliers, peu informés ou peu avertis, ou les organisations pour lesquelles la mise en place des correctifs, patchs de sécurité distribués par les éditeurs, peut poser un problème de compatibilité avec les logiciels existant de leur SI.

Ce contexte d'une recomposition incessante des outils numériques aboutit inévitablement à une augmentation des risques, qu'ils soient d'origine strictement technique ou liés à la malveillance. Ce constat est aggravé par la perspective d'une diffusion massive d'objets connectés dont la sécurité n'est généralement pas garantie ce qui va aboutir à une extension considérable de la ''surface d'attaque'' disponible pour les prédateurs du cyberespace.

Dans ces conditions, l'exception juridique du numérique que constitue l'absence de responsabilité du producteur sur son produit doit être reconsidérée.

L'exemple de Wannacry

En 2014, Microsoft avait indiqué qu'il stoppait le support technique de Windows XP. Cette décision était prévisible car directement issue de la politique de support technique de l'éditeur américain. Celui-ci assure généralement des mises à jour de ses logiciels durant dix ans. Passé ce délai, Microsoft invite ses utilisateurs à ''mettre à jour leur ordinateur avec un système plus récent ou à remplacer leur PC''. En 2014, un quart des PC français était encore équipés d'XP. A l'époque, la fin de la maintenance de ce système d'exploitation très répandu avait faire réagir une sénatrice française qui s'en était inquiétée.

Début 2017, Microsoft identifie et corrige une faille de sécurité qui concerne tous ses systèmes d'exploitation antérieurs à Windows 10. Un patch correctif est publié en mars mais celui-ci ne concerne pas XP mais seulement toutes les versions suivantes. Cette faille et le logiciel nécessaire à son exploitation sont révélés et diffusés en avril par un groupe de hackers qui les dérobe à la NSA.

En juin 2017, un logiciel malveillant de type ransomware auto-répliquant baptisé ''Wannacry'' utilise cette faille de sécurité lors d'une cyberattaque mondiale massive, touchant plus de 300 000 ordinateurs, dans plus de 150 pays. Parmi les plus importantes organisations touchées par cette attaque, on trouve notamment les entreprises Vodafone, FedEx, Renault, Telefónica, le National Health Service, le ministère de l'Intérieur russe ou encore la Deutsche Bahn.

Les failles de sécurité ne sont pas rares. Entre janvier 2007 et décembre 2016, 586 vulnérabilités de ce type ont été constatées sur des navigateurs Web

.

- **Affirmer la responsabilité des fournisseurs systémiques de produits numériques (hard ou soft) connectables sur la sécurité de leurs produits**

Aucun dispositif normé ne permet aujourd'hui de vérifier le niveau de sécurité des logiciels et applications proposés en grand nombre, éventuellement gratuitement, au grand public. Il n'existe pas de traçabilité des produits numériques, inatteignable du fait de leur recomposition incessante, or le secteur est dominé par un nombre restreint de **« fournisseurs systémiques »** dans les domaines des plateformes, des composants, des infrastructures, des systèmes d'exploitation, des solutions logicielles …

Dans ce secteur de grande consommation, le producteur met sur le marché des « objets » qu'il sait plus ou moins défaillants, et qui seront ensuite utilisables sans traçabilité en tant que « briques » (disponibles avec ou sans licence), y compris dans des domaines cruciaux ou connectés à des activités cruciales.

Dans le droit commun communautaire de la responsabilité civile, la responsabilité pour produit défectueux désigne « *l'obligation de sécurité du vendeur professionnel et plus largement du fournisseur professionnel, tenus de livrer un produit exempt de tout défaut de nature à créer un danger pour les personnes et pour les biens, sans qu'il y ait lieu de distinguer si les victimes avaient la qualité de parties contractantes ou de tiers (…) La responsabilité de plein droit du fabricant découle de la preuve du dommage, du défaut du produit, et du lien de causalité entre le défaut et le dommage (…)« L'insuffisante mention des effets indésirables possibles dans les documents établis à l'intention des utilisateurs* » peut être considérée comme un « *défaut extrinsèque du produit* » (Cour de Cassation).

En tout état de cause, le droit commun de la responsabilité civile ne prévoit pas d'exonération systématique pour risque de développement.

Or, dans des secteurs de diffusion comparable, tels que l'alimentation, l'automobile ou plus encore l'électricité, le producteur est responsable au civil et éventuellement au pénal de la sécurité et de la qualité de son produit. Pour chaque produit mis sur un marché BtoB ou BtoC, il existe en outre des normes européennes de fabrication garantissant la sécurité et un certain niveau de qualité des produits (incluant l'adaptation à l'usage revendiqué et la véracité des allégations) ainsi que, le plus souvent, des contrôleurs publics exerçant en amont et en aval de la mise sur le marché. Ainsi, jamais la sécurité du consommateur ou de l'utilisateur n'est censée reposer uniquement sur sa capacité propre à se protéger y compris via des prestataires privés, *a fortiori* dans un secteur où l'origine des composants des produits n'est pas traçable.

Pour stimuler la traçabilité des produits et ainsi réduire l'intensité de la menace, l'UE pourrait donc affirmer, comme condition d'accès à son marché, la responsabilité des fournisseurs systémiques, hard et soft, au titre des effets induits par leurs produits sur les objets et systèmes dans lesquels ils sont utilisés (réseaux, procédés, usages domestiques, …).

- **Examiner une condition d'assurabilité des produits pour la mise en marché**

Actuellement, les assureurs ne disposent pas de la totalité des éléments qui leur sont nécessaires en termes de données pour dimensionner leur offre cyber.

Le risque cyber est un risque qui affecte la valeur tangible de l'organisation mais également la valeur intangible que sont, pour partie, la confiance et la réputation. Cette valeur intangible va constituer une part de plus en plus importante de la valorisation de l'entreprise. Elle est évaluée par les auditeurs, les investisseurs, le régulateur et les agences de notation.

Ces acteurs vont demander aux entreprises de présenter, en toute transparence, les actions qui sont mises en œuvre pour maîtriser ces risques. Sous cette pression-là, les conseils d'administration vont demander qu'on leur expose la gouvernance qui a été mise en place pour gérer, non seulement le risque cyber sur le plan technique (et de conformité) mais également sur le plan de sa gestion financière par le département de la finance et donc par le risk manager.

Par ce biais-là, le risk manager est légitime pour travailler avec l'assureur pour déterminer quelles sont les conditions de couverture pertinentes par rapport à son besoin. Dans ce sens-là, les assureurs vont être un acteur de la valorisation de l'entreprise ce qui aujourd'hui n'est pas le cas.

Interroger les acteurs en charge de la valorisation des biens, et en particulier des biens intangibles, profitera au marché de l'assurance et permettra d'aider à l'élaboration des éléments financiers constitutifs d'une analyse de risque financière du risque cyber.

Le principe de l'assurance est de remettre l'assuré dans les conditions où il était avant le sinistre. Aujourd'hui, en matière d'attaque cyber des progrès sont à faire pour arriver à ce résultat (contrairement aux aléas traditionnels incendies et vols) alors que la résilience ou l'anti-fragilité réclament une situation améliorée après sinistre.

Pour dimensionner leur offre cyber, les assureurs ont besoin d'avancer sur deux thèmes : quantifier le risque cyber, en particulier celui relatif aux biens intangibles et comprendre comment va s'organiser la gouvernance du risque cyber et quels en sont les attendus par les acteurs de la valorisation de l'entreprise.

Ce sujet est a fait l'objet d'une étude portée par l'Institut de recherche technologique SYSTEM X (Maîtrise du risque cyber et son transfert vers l'assurance)

L'implication des assureurs sur ce sujet les conduira par ailleurs à développer un réseau d'expertises qui , comme sur les autres risques, aidera leurs clients à diminuer leur exposition aux risques pour réduire leurs primes.

Recommandation n°7 - Réglementer et réguler pour réduire les risques

❑ Objectifs et modalités

Action 1 : Intégrer dans l'économie numérique le principe de responsabilité des fournisseurs systémiques. Supprimer ou restreindre l'exception du numérique dans ce domaine

Action 2 : **Pour favoriser l'assurabilité du risque cyber , mettre en place un dispositif de co-working entre assureurs, commissaires aux comptes, acteurs privés et puissance publique pour renforcer l'offre du marché de l'assurance de la cyber sécurité.**

❑ Impact attendu

Amélioration radicale de la sécurité des produits du marché

❑ Conditions de réussite

Mobilisation de la Commission Européenne , notamment par la poursuite du travail sur la certification européenne de sécurité

Prise en compte des travaux de l'IRT System X « LA MAÎTRISE DU RISQUE CYBER SUR L'ENSEMBLE DE LA CHAÎNE DE SA VALEUR ET SON TRANSFERT VERS L'ASSURANCE » , en évaluer la dynamique

❑ Ressources à mobiliser

Action 1: moyens pour agir auprès de la Commission européenne (2 ETP);

Action 2: assez faibles pour l'Etat, mais important pour les acteurs . Solliciter le Conseil d'Etat la Fédération Française de l'Assurance, la Compagnie Nationale des Commissaires aux Comptes, les avocats spécialisés

❑ Services en charge de la mise en œuvre

Action 1 : Le CGE conduit une étude complémentaire sur le sujet en 2018

Action 2 : DGT (porteur) ou DGE , Fédération Française de l'Assurance, Compagnie Nationale des Commissaires aux Comptes, ANSSI

Synthèse

Liste des recommandations

Les attaques dans le cyber-espace sont de plus en plus fréquentes et sophistiquées, la défense ne suffit plus à assurer la survie des organisations

Les points essentiels pour réduire les risques et les impacts

Les actions proposées

Annexes

Aller au sommaire

Aller au sommaire

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CONSEIL GÉNÉRAL DE L'ÉCONOMIE
DE L'INDUSTRIE, DE L'ÉNERGIE ET DES TECHNOLOGIES
TELEDOC 792
BATIMENT NECKER
120, RUE DE BERCY
75572 PARIS CEDEX 12

Affaire suivie par : Françoise Roure
Téléphone : 01 53 18 56 87
Télécopie: 01 53 18 57 15
Mél. : francoise.roure@finances.gouv.fr
Dossier N° 331

Paris, le 10 FEV. 2017

Le Vice-président

à

M. Marc MEYER
Ingénieur général des mines

M. Laurent de MERCEY
Ingénieur général des mines

M. Yves MAGNE
Administrateur civil HC

Objet : Thème d'approfondissement de la section *Sécurité et risques* pour l'année 2017.

La généralisation de la transformation numérique à l'ensemble des activités, économiques, sociales, personnelles conjuguée avec son approfondissement et sa complexification (*cloud computing, big data* notamment) conduisent à de nombreuses opportunités pour les personnes, les organisations, les Etats et les territoires.

Dans le même mouvement d'ensemble, les risques cyber touchant la sécurité et la sûreté se multiplient et s'aggravent tant en ce qui concerne les individus que les groupes, les organisations ou les territoires, avec des coûts croissants et une assurabilité partielle. Les Etats, sur leur propre territoire, peinent à assurer leur pleine souveraineté législative, exécutive et judiciaire sur les activités numériques. L'application du droit public international reste largement à préciser et à mettre en œuvre dans le cyberespace.

Dans ce contexte, la cyber résilience concerne autant les traitements informatiques et les processus que la préservation des données. Elle peut être définie comme la capacité de rétablir un fonctionnement satisfaisant, tout notamment des outils numériques, après des attaques délibérées, des accidents ou des catastrophes naturelles. Cette capacité est susceptible d'avoir été mise en difficulté par la rapidité de la transformation numérique de notre économie et le caractère systémique des risques numériques, sans que les réponses en termes de sûreté ne l'aient suivie. A l'inverse l'imbrication entre le monde numérique et le monde réel améliore considérablement la résilience globale.

C'est pourquoi le Conseil a décidé que la section *Sécurité et risques* sera chargée d'approfondir ce sujet dans le cadre de son programme de travail 2017.

Compte tenu des enjeux économiques et financiers, techniques et sociétaux de la cyber résilience, je souhaite que vous étudiiez les questions suivantes :

- Quel est l'état des lieux des vulnérabilités cyber, dans les entreprises et les secteurs d'importance vitale pour la société et la vie quotidienne y compris à la maille de certains territoires?
- Quelles sont les menaces cyber les plus critiques au regard de ces vulnérabilités ?
- Quelles politiques et parades de cyber résilience, les pouvoirs publics peuvent-ils définir et mettre en œuvre, ou faire mettre en œuvre, efficacement, de façon unilatérale, coopérative ou multilatérale ?
- Comment utiliser le levier des acteurs français, notamment des laboratoires de recherche et des entreprises, pour apporter des solutions de nature à renforcer la résilience systémique et à améliorer notre compétitivité internationale?

Conformément à l'organisation des travaux d'approfondissement des sections, je vous désigne, sur proposition du président de la section SR, rapporteurs de cette mission d'analyse et de conseil. Vous prendrez tous les contacts utiles auprès des administrations, services de l'Etat et collectivités publiques, et des experts privés ou académiques. Vous vous efforcerez de répondre aux questions posées plus haut, en établissant des constats objectifs et chiffrés, et en formulant des propositions concrètes et opérationnelles.

En termes d'étapes :

- vous élaborerez d'ici mi mars 2017 une note de cadrage visant à affiner le périmètre de la mission, en proposant un ciblage provisoire de vos travaux sur une partie pertinente et stratégique du cyberespace. Vous veillerez particulièrement à cet égard à proposer d'inscrire vos travaux en complément de qui est assuré par les ministères, notamment ceux chargés de l'intérieur, de l'énergie, des transports et de l'économie, de la santé, et les organismes interministériels pertinents tels le SGDSN ;
- dans un second temps, vous vous attacherez à présenter une cartographie des vulnérabilités de la résilience de cette partie du cyberespace, faisant apparaître une vision synthétique de ces vulnérabilités et des menaces, ainsi que de leurs évolutions, sous la forme d'un rapport d'étape qui me sera remis pour juillet 2017 ;
- enfin, vos travaux donneront lieu pour fin 2017 à un rapport avec des propositions d'actions opérationnelles des ministères, de leurs établissements publics et de leurs services déconcentrés en matière de cyber résilience.

En termes de méthode :

- vous rendrez compte à la section de l'avancée de vos travaux et de la suite que vous envisagez d'y apporter ;
- vous ouvrirez le débat avec vos collègues de la section sur vos constats, vos interrogations et vos propositions ;
- enfin, vous pourrez vous rapprocher du président suppléant de la section SR que je désigne, conformément aux dispositions du *Guide de procédures pour la conduite des missions d'expertise et de conseil*, comme *challenger* de cette mission.

Luc ROUSSEAU

Copies : Mme la présidente de la section SR
M. le président suppléant de la section SR

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

2/2

Aller au sommaire

Déroulement de la mission

Mars / Avril 2017
- cadrage de la commande par la mission; rencontre SGDSN / ANSSI et HFDS (MTES, Bercy), DGE, Mindef, MISC
- état des lieux des politiques conduites dans le domaine de la cyber-sécurité et de la cyber-résilience

Mai / Juillet 2017
- rencontre d'une cinquantaine d'entités publiques ou privées
- constitution d'une bibliographie

Juin / Juillet 2017
- présentations en section SR et premières contributions
- élaboration de monographies (énergie, secteur financier, transports)

Septembre 2017
- intervenants en section: Cotelle (Airbus), Abitboul (INRIA), Caurette (ACN), Coustillière (Mindef)
- remise du rapport intermédiaire d'étape « état des lieux » de la cyber-résilience en France et dans le monde

Octobre 2017
- rencontres en bilatéral de membres de la section avec deux objectifs: compléter / valider l'état des lieux et préparer les recommandations

Novembre 2017
- présentation des recommandations en section, débat, lancement d'un questionnaire
- début de rédaction du rapport final en deux parties: points clefs issus du rapport d'étape et qualification des recommandations

Décembre 2017
Janvier 2018
- rencontre des acteurs clefs pour mettre les recommandations en débat
- finalisation des recommandations pour fin janvier 2018

Aller au sommaire

La mondialisation d'internet a vu l'émergence de la cybercriminalité presque partout où la connexion est possible. Celle-ci a pris des formes très diverses et, en dépit de son caractère transnational, des facteurs socioculturels et économiques parfois forts restent prégnants dans les méthodes et les attitudes des cybercriminels. Ils ont pu être renforcés par le prolongement dans le cyber-espace des conflits politiques du monde physique, ce qui est devenu presque la règle depuis une dizaine d'années. Trois grands pays voient leurs hackers dominer le cyber-espace : les Etats-Unis, la Chine et la Russie. D'autres, de plus en plus nombreux, développent des capacités offensives et mettent en place des unités constituées de cyber-soldats. C'est en particulier le cas de l'Iran, de la Corée du Nord et d'Israël. En Europe, le Royaume Uni n'est pas en reste et tire parti de ses relations privilégiées avec les Etats-Unis en matière de renseignement électronique.

- **Les hackers d'Europe de l'est**

La cybercriminalité russe est hors norme, tant par le niveau de ses hackers, souvent très experts mais volontiers solitaires, par les caractéristiques de son « marché », très dynamique et porté par la revente de données volées, en particulier bancaires, par ses relations très opaques avec certains organes officiels russes et ses liens avec des courants nationalistes qui ont été très actifs contre la Géorgie, l'Estonie ou l'Ukraine. Deux groupes de hackers russes font beaucoup parler d'eux depuis quelques années, dénommées APT 28 ou Cosy Bear et APT 29 ou Fancy Bear, ils sont notamment été accusées d'avoir commis les attaques contre TV5 Monde ou le Bundestag en 2015 et, en 2016, d'avoir détourné des données du comité national du parti démocrate lors des élections présidentielles américaines.

Autre héritage historique, celui de la qualité de l'apprentissage des mathématiques en Russie qui demeure à un haut niveau aujourd'hui et favorise fortement la maitrise de la programmation informatique. Les hackers russes sont reconnus comme étant particulièrement brillants. Cette réputation n'est pas surfaite, puisqu'ils sont parmi les premiers producteurs de virus et autres malwares vendus ensuite au reste du monde sur les places de marché du darkweb. Cette activité économique particulièrement rentable renvoie à la situation des chercheurs, ingénieurs et techniciens de l'époque soviétique, brutalement privés d'emploi par l'effondrement de l'URSS, et pour lesquels l'informatique a constitué une source de revenu de substitution.

Les hackers d'Afrique de l'Ouest

En quelques années, la cybercriminalité s'est fortement développée en Afrique de l'Ouest. Parmi les facteurs qui peuvent l'expliquer, le premier est économique. Le taux de chômage des jeunes diplômés dans la région avoisinerait les 50%. La cybercriminalité séduit en raison de l'importance des gains qu'elle rapporte et d'un certain prestige social qui peut lui être associé parmi la jeune génération. Elle est également encouragée par une indulgence culturelle à l'égard de l'escroquerie, dès lors que la pauvreté la justifie, ainsi que par le ressentiment à l'égard des anciens colonisateurs qui peut inciter à recouvrir une ''dette coloniale'' en ciblant ces derniers. Le Nigéria est le pays où elle est le plus développée mais la Côte d'Ivoire n'est pas en reste et ses hackers ciblent les pays francophones. La majorité d'entre eux n'a que de faibles compétences techniques mais excellent en matière d'ingénierie sociale en réalisant des escroqueries variées et régulièrement renouvelées : demandes d'avance pour transférer des fonds ou pour faire face à une situation d'urgence, le cas échéant en usurpant une identité, faux héritages ou prêts bancaires nécessitant une « garantie » pour débloquer l'argent, relations sentimentales intéressées, chantage à la vidéo compromettante, ces petits escrocs surnommés les ''brouteurs'' rivalisent d'ingéniosité pour gruger leurs victimes. Une proportion restreinte des hackers ouest-africains accède à des niveaux techniques plus élevés qui leur permettent de réaliser des fraudes financières à l'étranger, pour l'essentiel en achetant sur des places de marché des outils de hacking comme ceux nécessaires au phishing, au cryptage de données, à l'espionnage ou à la prise de contrôle à distance. Ils se dotent de capacités de blanchiment d'argent et ouvrent des comptes bancaires à l'étranger. Généralement plus âgés que les brouteurs, ils sont également plus discrets et n'exposent pas leurs gains ostensiblement alors que ceux-ci sont bien supérieurs à ceux de la jeune génération. Il n'existe pas encore de place de marché spécifique à l'Afrique de l'Ouest, mais le milieu des hackers se caractérise par un niveau d'échange et de collaboration très élevé localement.

Les hackers asiatiques

Selon le Département d'Etat américain, l'équivalent chinois de la NSA compterait plus de 100 000 personnes. Au sein de la structure, des unités sont dédiées aux actions d'espionnage. Certaines ont des compétences géographiques, comme c'est le cas de l'unité 617398 qui est spécialisée sur les Etats-Unis et le Canada, ou l'unité 61486 dont le domaine est l'Europe. L'essentiel de l'activité de ces structures est destiné à l'espionnage économique et industriel, ce qui a valu à la Chine d'être mise en cause lors des vols massifs de données qui ont concerné principalement des pays de langue anglaise ; toutefois la France n'a pas été épargnée. Les groupes de hackers chinois ont sans doute été les plus prolifiques au monde en termes de quantité d'informations volées. Cette activité semble avoir nettement décliné depuis la signature d'un accord sino-américain en 2015 destiné à mettre un terme à l'espionnage industriel et commercial dans le cyber-espace entre les deux pays. Dans le même espace, les actions offensives hors du champ de l'espionnage apparaissent beaucoup plus rares que celles des Russes. Les hackers chinois privilégient la discrétion dans leurs actions. Un attaque du dépôt de logiciels libres ''Github'', par déni de service en 2015, a cependant été plus ou moins attribuée au gouvernement chinois, le site en question accueillant entre autres des développements de logiciels destinés à contourner la censure d'internet par ces autorités.

Il semble donc bien que les hackers chinois soient majoritairement, recrutés parmi les jeunes diplômés en informatique avec comme mission prioritaire l'espionnage économique et industriel.

Aucune étude précise ne permet d'évaluer la part de cybercriminalité chinoise en provenance de la diaspora ou ses liens mais ses hackers semblent avoir pris l'habitude de lancer leurs attaques à partir de pays étrangers afin de masquer leur nationalité. Cela a pu leur valoir des réactions policières de l'Indonésie, notamment, qui a arrêté et expulsé à plusieurs reprises des hackers chinois venus sur son territoire pour y mener des activités illégales.

Les hackers américains

En 2012, l'Amiral Keith Alexander, alors directeur de la NSA, fit une apparition remarquée lors de DEFCON à Las Vegas, en appelant ''la meilleure communauté mondiale de cybersécurité « à venir travailler pour la NSA ». Pour cette agence, comme pour tous les services officiels ou les entreprises privées spécialisés en cybersécurité, le recrutement d'experts de haut niveau est vital, mais, aux Etats-Unis comme ailleurs, la ressource manque. Il s'agit donc de recruter les meilleurs codeurs ou cyber-experts, où qu'ils se trouvent.

Depuis l'affaire Snowden en 2013, il faut constater que les informations concernant les hackers américains, qu'ils soient indépendants, issus des services officiels ou des entreprises privées, sont particulièrement limitées. Les principales entreprises mondiales du secteur sont américaines, les laboratoires de recherches les plus avancés le sont aussi, les budgets américains destinés à la cyberdéfense sont certainement les plus importants au monde et en croissance permanente. En revanche, la législation et les sanctions contre le hacking ont été régulièrement et lourdement renforcées depuis des années. Les activités indépendantes dans ce domaine sont devenues très risquées aux Etats-Unis.

Les révélations effectuées par WikiLeaks sous le nom de code Vault 7 au début 2017 démontrent que les services américains ont su constituer un arsenal d'outils de hacking impressionnant. Il permet notamment de compromettre la plupart des systèmes d'exploitation d'ordinateur ou de smartphone ainsi que les navigateurs web, de masquer et brouiller les pistes après une attaque informatique, de prendre le contrôle de certains véhicules ou de téléviseurs… Symantec indiquait, en 2008, que les États-Unis abritaient 42% des serveurs de contrôle et de commande des bots et que 37% des attaques mondiales provenaient de ce pays. Cette société n'a plus diffusé ce type de chiffres depuis cette date.

Les hackers d'Europe occidentale

Une enquête de la police britannique donne quelques éclairages intéressants sur les profils des cybercriminels au Royaume Uni. Ceux-ci sont particulièrement jeunes, 17 ans en moyenne, ne relèvent pas d'une catégorie sociale particulière et ont généralement accédé à la cybercriminalité par les jeux vidéo. C'est en apprenant à modifier et à personnaliser ces jeux grâce à des conseils et des informations diffusées sur des forums qu'ils vont progressivement développer des activités illégales. Cette dérive est facilitée par l'accessibilité des outils de hacking, disponibles sur internet et simples à utiliser. Des vidéos permettent d'en apprendre l'usage pour des utilisateurs dont le niveau technique est généralement assez bas. Seul un petit nombre d'entre eux va accéder à un niveau plus élevé de compétences techniques nécessaires à des activités de cybercriminalité élaborées. Une proportion importante de cette population, n'a que faiblement conscience du caractère illégal de ses actions, de leurs conséquences et du risque de poursuite encouru. L'absence de présence visible des services de police sur la toile et l'anonymat apparent, mais trompeur, de ces activités semblent expliquer ce sentiment. Les questions juridiques et leurs conséquences sont rarement évoquées sur les forums de hackers. Leur première motivation n'est pas nécessairement financière. Il s'agit bien souvent de relever un défi, de démontrer ses qualités en accomplissant une action difficile pour renforcer l'estime de soi ou d'obtenir celle de ses pairs. Les relations sociales, les interactions, même en ligne, sont essentielles pour expliquer l'engagement des jeunes cybercriminels.

Le portrait-robot du jeune hacker réalisé par la police britannique, n'est probablement pas éloigné de celui de son équivalent français. Une différence importante semble toutefois les séparer, les hackers français apparaissent beaucoup plus prudents sur les réseaux et le darkweb où la peur du gendarme marque les comportements. Un point en revanche semble les rassembler, ces cyber-délinquants ne sont pas prédisposés à la criminalité ordinaire et ne participent guère aux grands réseaux de la criminalité organisée internationale.

Les hackers liés au terrorisme ou à la criminalité organisée traditionnelle

Il semble bien que ce constat concerne également dans une bonne mesure les pratiques des organisations terroristes djihadistes. Si elles ont engagé certaines actions relevant du domaine du code, celles-ci ont été limitées à des opérations relativement simples comme le piratage de compte Twitter ou le défacement (maquillage) de sites internet. Ainsi que l'indique Damien Bancal « Les présumés pirates informatiques de Daesh sont avant tout de « simples » petits criminels évoluant dans le blackmarket et le hack facile. Ce ne sont pas des professionnels ». En outre, il semble que des sympathisants de l'organisation en soient à l'origine, plutôt que les cyber-terroristes directement liés à l'Etat Islamique. Ces derniers paraissent se consacrer avant tout à la propagande, au recrutement ou aux circuits financiers de l'organisation.

Jusqu'à présent, si les grands réseaux criminels « classiques » comme les groupes terroristes ont largement eu recours aux outils et ressources disponibles sur l'internet ouvert ou le darkweb, essentiellement dans la couche sémantique du cyber-espace, il ne semble pas qu'ils aient produit à leur niveau des outils élaborés pour leurs besoins propres. La cybercriminalité de haut niveau ne se serait donc pas réellement interpénétrée avec les réseaux criminels classiques ou terroristes. Ces organisations n'ont pas, ou pas encore, développé des modes d'action visant à coordonner des interventions dans le monde physique et des actions dans le cyber-espace au moyen d'outils logiciels.

Cette course à l'armement cyber ne peut qu'alimenter l'inquiétude. Il sera évidemment beaucoup plus difficile d'empêcher la prolifération de lignes de code que de matériels militaires lourds et il parait inévitable que certaines de ces armes échapperont au contrôle de leurs fabricants et iront rejoindre les arsenaux privés des criminels ou des terroristes. La divulgation malencontreuse par la NSA de la faille de sécurité qui a ensuite été exploitée par le rançongiciel WannaCry est révélatrice à cet égard.

Les risques systémiques du cyber-espace : une problématique encore émergente

La notion de risque systémique a été fréquemment évoquée pour le secteur financier. Elle correspond à un événement à l'origine de pertes économiques importantes ou d'une perte de confiance, ce qui suscite des inquiétudes sur la situation d'une partie importante du système financier, suffisamment sérieuses pour avoir des effets négatifs sur l'économie réelle. La définition qui pourrait en être faite pour ce qui concerne le cyber-espace doit évidemment être plus large. Elle doit inclure la dimension humaine, la part de confiance nécessaire dans le fonctionnement des outils numériques dont l'importance est toujours grandissante et qui sont souvent irremplaçables dans la plupart des secteurs d'activités. Le meilleur des systèmes perd une part essentielle, voire la totalité de son utilité si sa fiabilité est mise en cause, y compris à tort. Mais cette définition doit également prendre en compte la dimension strictement technique, l'hypothèse d'une panne qui provoquerait l'effondrement en série des outils et services d'un domaine plus ou moins étendu. Pour revenir au secteur financier, le risque systémique est parfois envisagé pour ce qui concerne le trading de haute fréquence, ces transactions entièrement automatisées qui ont un effet décisif sur les marchés, sans intervention humaine. La question se pose de savoir quelles pourraient être les conséquences d'une panne imprévisible, d'un dysfonctionnement non détecté, d'une manipulation ou d'une attaque délibérée sur le système et quels seraient alors les impacts sur l'économie réelle. Le système des cartes bancaires de par sa dimension et sa très large utilisation est également vulnérable à une attaque de grande ampleur. Deux autres domaines font déjà l'objet d'une préoccupation quant à la possibilité d'un risque systémique.

Celui de l'énergie, ce qui a été illustré par exemple lors de la cyber-attaque sur plusieurs opérateurs électriques ukrainiens en décembre 2015 qui a provoqué des coupures importantes et une remise en fonction laborieuse. C'est la première fois qu'une attaque informatique visant spécifiquement un réseau électrique parvenait à ses fins. Tous les experts s'accordent cependant pour constater que le degré de préparation, de coordination, de connaissance des systèmes industriels visés, ainsi que les moyens financiers probablement engagés dans cette opération ne sont pas à la portée de tous les groupes criminels ni de tous les Etats. Mais, à l'inverse, la comparaison entre les réseaux d'Ukraine et d'Europe occidentale n'incite pas à un optimisme excessif. Le réseau français, plus moderne et davantage automatisé que le réseau ukrainien, parait davantage exposé à une cyber-agression. En outre, les moyens d'action pour se prémunir de ce type de menace au niveau européen sont encore très limités alors que les infrastructures énergétiques des pays de la zone sont de plus en plus interconnectées, ce qui multiplie les vulnérabilités et les points d'attaque possibles. Pour l'heure, ni l'ENISA, agence en charge de la sécurité des réseaux et de l'information au niveau européen, ni l'ENTSOe qui coordonne les GRT ne sont en mesure de faire appliquer des normes communes en matière de sécurité des systèmes d'information. Cette situation n'est pas spécifique au secteur de l'énergie.

Le domaine de la « ville intelligente » suscite également des interrogations. Un groupe de travail de l'Union Européenne constate en effet que les infrastructures critiques modernes deviennent toujours plus « intelligentes » dans leur fonctionnement sous l'effet de l'automatisation logicielle et robotique, et grâce à l'exploitation des données. Pour autant, la question de leur résilience se pose dans l'hypothèse d'une menace hors normes comme une catastrophe climatique ou d'une attaque terroriste. Il s'agit également de savoir si la complexité qui accompagne le gain en intelligence de ces infrastructures ne les rend pas plus vulnérables. Le groupe de travail s'est donné pour objectif d'établir des métriques destinées à évaluer le niveau de résilience des infrastructures dans des conditions extrêmes.

Du coté des assureurs, la couverture du risque cyber progresse mais elle butte sur le scénario où une grande partie des assurés serait affectée par une même attaque à grande échelle, générant un besoin d'indemnisation trop important pour que l'assureur soit en mesure d'y répondre. Les récentes attaques des malwares WannaCry et NotPetya ont démontré que cette hypothèse était des plus sérieuses.

Aller au sommaire

Les différentes catégories de cyber-attaques

Les modes d'action des prédateurs du cyber-espace sont particulièrement nombreux et en perpétuelle évolution. Parmi les plus connus et les plus utilisés, les dispositifs d'attaque par déni de service, les attaques en profondeur, les malwares et virus, les e-mails piégés.

Le déni de service : une arme multi usages

L'attaque par déni de service (Distributed Denial of Service - DDoS) vise à paralyser le fonctionnement d'un serveur informatique en le saturant par un grand nombre de requêtes. L'effet est décuplé par le recours à des réseaux d'ordinateurs « zombies » ou « botnet » qui vont chacun solliciter le serveur. Ces machines, qui ont été préalablement infectées à l'aide d'un logiciel malveillant, sont commandées à distance par les pirates.

Le nombre de ces attaques n'a cessé de croitre au cours des vingt dernières années. Considérées par les experts en sécurité comme une tendance majeure en 2017, elles se caractérisent par leur ampleur, leur fréquence et leur sophistication grandissante.

Il s'agit d'une arme à usages multiples utilisable pour des représailles ou du chantage. Contrairement à la plupart des autres outils de hacking, sa mise en œuvre n'est pas discrète. Ce type d'attaque est fréquemment utilisé dans un contexte politique où sa capacité de démonstration de force est recherchée. Ce fut le cas contre la Géorgie, l'Estonie ou l'Ukraine, des hackers russes ayant réussi à bloquer l'accès des sites internet officiels de ces pays. Elle a également été employée contre le secteur bancaire aux Etats-Unis en 2012, sans doute depuis l'Iran, et contre le dépôt de logiciels libres ''Github'' par des hackers probablement chinois en 2015.

Si certains services d'Etat ou associés l'utilisent régulièrement, ce mode d'action est également très pratiqué par des cybercriminels recherchant le profit. Il s'agit alors de lancer une attaque contre une entreprise ou un service en ligne puis de lui réclamer de l'argent pour y mettre fin. Une pratique très répandue consiste également à louer un botnet pour mener l'opération. Pour quelques dollars de l'heure, ce genre de dispositif se trouve facilement sur les places de marché du darkweb.

Une « innovation » réalisée par un hacker indépendant en 2016 a permis d'augmenter considérablement l'efficacité de ce type d'attaque. Ce dernier a créé un malware nommé Mirai destiné à prendre le contrôle de botnets et qui a la particularité de cibler principalement des objets connectés tels que des caméras pilotables à distance ou encore des routeurs. Généralement, les objets connectés sont peu ou pas sécurisés, ce qui donne à ce malware une grande efficacité pour constituer des botnets particulièrement puissants car rassemblant un grand nombre de bots. Un ou plusieurs botnets Mirai ont été utilisés en 2016 pour des attaques d'une ampleur sans précédent qui ont notamment touché l'hébergeur français OVH et la société Dyn, un important fournisseur de noms de domaine.

Malwares et ransomwares – un arsenal disponible en croissance permanente

Les virus et logiciels malveillants (malwares) remontent aux premiers temps du hacking mais ils continuent de représenter une des premières menaces du cyber-espace. Depuis ces dernières années, les capacités de destruction et de ciblage des versions les plus récentes ont fortement augmenté, ce qui justifie l'inquiétude des pouvoirs publics et relance les spéculations sur un possible ''cyber Pearl Harbor'' face à l'ampleur des dégâts constatés et aux hypothèses d'attaques ultérieures.

Il existe une grande variété de virus et malwares puisque chaque hacker de bon niveau va produire les siens mais le plus souvent en s'inspirant de l'existant qu'il va modifier ou combiner selon ses propres besoins. Chaque diffusion d'un nouveau malware contribue donc à enrichir l'arsenal de tous les hackers.

Le cas de WannaCry en mai 2017 a révélé au grand public l'existence des logiciels malveillants de type ransomware auto-répliquant en provoquant le plus grand piratage à rançon de l'histoire d'Internet. Cette cyberattaque mondiale massive a touché plus de 300 000 ordinateurs dans plus de 150 pays en utilisant une faille de sécurité nommée ''EternalBlue'' du système Windows XP exploitée par la NSA et volée en 2016 par les Shadow Brokers, un groupe de pirates informatiques. Cette faille avait été corrigée en mars 2017 par Microsoft, mais cela n'a pas suffi à éviter qu'elle provoque un grand nombre de victimes. Parmi elles, de grandes entreprises comme Vodafone, FedEx, Renault, Telefónica, mais aussi le National Health Service britannique dont une vingtaine d'hôpitaux a été touchée, le ministère de l'Intérieur russe ou encore la Deutsche Bahn. L'étendue des dégâts causés par WannaCry ainsi que la rapidité de sa propagation ont impressionné les experts. Ceux-ci demeurent interrogatifs quant à l'origine du malware. Les soupçons qui visent la Corée du Nord ou des hackers chinois n'ont pas été confirmés et la véritable motivation de l'opération n'est pas établie.

Un autre malware a rapidement suivi WannaCry en juin 2017. NotPetya semblait s'en rapprocher mais il est rapidement apparu que son objectif était différent et son ciblage plus précis. Ce malware vise en particulier les organisations et entreprises d'Ukraine ou celles qui collaborent avec elles. Son objectif n'est pas financier, ce logiciel n'est pas un rançongiciel, même s'il Il est prévu pour effacer automatiquement les données des ordinateurs contaminés.

Les effets de NotPetya ressemblent à ceux du virus Shamoon qui avait détruit 35 000 postes de travail de la compagnie saoudienne Aramco en 2012. La nouveauté de NotPetya réside dans sa capacité à se diffuser dans une zone d'influence politico-économique, en l'occurrence celle de l'Ukraine, alors que Shamoon ne visait qu'une entreprise. Pas plus que pour WannaCry, l'impact économique global de NotPetya n'a été évalué mais cette attaque a coûté plusieurs centaines de millions d'euros à Saint-Gobain.

Si les auteurs de ces différentes attaques sont certainement liés à des Etats et agissent pour des motifs essentiellement politiques, les ransomwares trouvent également des utilisateurs parmi les cybercriminels dont les objectifs sont strictement économiques. Ce type de malware peut en effet agir en deux temps, en doublant leur profit. Tout d'abord en permettant le vol de données confidentielles qui peuvent ensuite être revendues, puis en cryptant ces données pour extorquer une rançon à leur propriétaire.

Les attaques en profondeur ou menaces persistantes avancées (Advanced Persistent Threats - APT)

Une ''Advanced Persistent Threat'' est un type de piratage informatique furtif et continu essentiellement destiné à l'espionnage ou à l'intelligence économique, ciblant généralement une organisation publique ou privée pour des motifs économiques ou un État pour des motifs politiques. Elle cible généralement des institutions et des industriels œuvrant dans des secteurs sensibles comme la défense, le nucléaire, l'énergie, l'aéronautique, le spatial, la diplomatie mais aussi des secteurs porteurs dans lesquels l'innovation est capitale : pharmaceutique, chimie, robotique.

Une APT exige un degré élevé de dissimulation sur une longue période de temps. Le but d'une telle attaque est de positionner du code malveillant personnalisé sur un ou plusieurs ordinateurs pour effectuer des tâches spécifiques tout en restant invisible pendant la plus longue période possible. Il s'agit de menaces sophistiquées et redoutées car elles combinent souvent différents vecteurs et stratégies d'attaques pouvant utiliser des techniques inconnues ou des failles ''zero day'' sans être détectées durant de longues périodes. Quand elles finissent par l'être, ce qui est loin d'être systématique, il est généralement très difficile d'en identifier l'origine.

Les APT nécessitent un niveau technique très élevé de la part des agresseurs et une capacité de planification élaborée. Il s'agit d'opérations complexes conduites sur des durées longues et dont les modes d'action vont évoluer en fonction de l'avancement de l'attaque, du contexte de l'attaquant qui sera progressivement découvert et des difficultés rencontrées au fil du temps. Elles exigent un savoir-faire assez rare dans le monde du hacking et sont réservées à une mince élite de cybercriminels qui travaille généralement pour le compte d'un Etat.

La première attaque de ce type, l'opération ''Titan Rain'' qui visait essentiellement des centres de recherche, des entreprises et des organisations officielles américaines, a été découverte en 2003. Elle aurait duré environ 3 ans. L'entreprise française AREVA a découvert en 2011 qu'elle avait été victime d'intrusions depuis plus de deux ans. L'ampleur du préjudice qu'elle a subi en termes de vol d'informations et de données touchant ses secrets industriels n'est pas connue, mais elle est certainement substantielle. Parmi les APT de grande ampleur, l'opération ''Aurora'', qui a été découverte par Google en janvier 2010 ciblait plus d'une trentaine d'entreprises de haute technologie et d'internet comme Adobe, Juniper Networks, Yahoo, Symantec, Northrop Grumman. Elle a provoqué un incident diplomatique avec le gouvernement chinois, ce dernier rejetant les accusations que la presse américaine avait lancées sur deux écoles chinoises spécialisées en informatique qui auraient pu être à l'origine de l'attaque.

Fraudes utilisant l'e-mail

A l'opposé des utilisateurs d'APT, les hackers utilisateurs d'e-mail sont très nombreux car les techniques utilisant la messagerie des entreprises sont simples et les potentiels de gains élevés.

La ''fraude au président'' ou ''Business Email Compromise'' est une des plus efficaces. Elle consiste à l'envoi par e-mail d'un faux ordre de virement international au service financier d'une entreprise. En dépit des mises en alerte abondamment diffusées par les services officiels et les médias, ce type d'escroquerie est en forte augmentation et les gains qu'il permet sont élevés. Une telle attaque pour un montant de 5 M€ a récemment failli aboutir auprès du CBCM du ministère chargé des finances. La banque centrale d'Indonésie a connu un scénario similaire qui lui a coûté 80 M€.

D'autres types d'escroquerie utilisent également l'e-mail, comme l'hameçonnage (phishing) qui permet de collecter des coordonnées bancaires, des informations personnelles ou des mots de passe. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance - banque, administration, service d'une entreprise - afin de lui soutirer les informations recherchées grâce à un message dont la présentation correspond à celle du site internet du tiers en question. L'e-mail est également l'une des voies les plus simples pour installer un malware sur un ordinateur en le transmettant en pièce jointe d'un message.

L'e-mail est par ailleurs un outil indispensable de l'ingénierie sociale et de l'escroquerie de petit niveau technique comme le pratiquent les hackers africains avec une grande efficacité.

Personnes ou secteurs concernés	Domaines de vulnérabilité et fonctions essentielles à préserver	Menaces
Particuliers	- - Les données personnelles : - - données bancaires ou administratives - - données professionnelles, pour les travailleurs indépendants ou mobiles - - les données personnelles à caractère intime dont l'importance est sentimentale ou qui peuvent engager la réputation - - L'accès aux services essentiels - - Accès à l'eau et l'alimentation - Accès à l'électricité - Accès à la Santé Mobilité : pouvoir se déplacer Pouvoir communiquer, échanger, maintenir les liens sociaux Disposer d'une information de qualité, complète, accessible et objective	- Blackout électrique. - Escroquerie par hameçonnage, vol de données, de mots de passe, ingénierie sociale. - Diffusion non volontaire ou non maitrisée de données. - Panne ou perte de matériel avec perte de données. - Dépendance commerciale excessive à l'égard d'un éditeur, d'antivirus par exemple, ou d'un cloud. - Atteinte à la réputation par les réseaux sociaux. - Cyber harcèlement - Manipulation, désinformation.
Entreprise	Fonctions essentielles qui font la raison d'être de l'entreprise et en particulier : - Production matérielle ou de services. - Mobilité indispensable à l'activité. - Relation avec les clients. Le cas échéant, interopérabilité et échanges avec les partenaires extérieurs de l'entreprise étendue. - Réputation de l'entreprise - Pour certaines (OIV) : - - Fourniture d'eau et d'alimentation - Fourniture d'électricité - Fourniture de santé - Banques : fourniture de liquidité	Les menaces dépendent de la taille des entreprises. Pour les TPE, les menaces correspondent en grande partie à celles qui concernent les particuliers. Pour les autres : - Blackout électrique. - Attaque sur la couche physique : infrastructures, réseaux physiques. - Attaque par déni de service. - Escroquerie par hameçonnage, vol de données, de mots de passe, compromission d'email, compromission de processus interne. - Ingénierie sociale. - Diffusion non volontaire ou non maitrisée de données, perte de données. - Externalisation trop poussée ou mal maitrisée, dépendance excessive à l'égard d'un éditeur, de PGI ou de base de données par exemple, ou d'un cloud. - Atteinte à la réputation par les réseaux sociaux ou les médias. - Manipulation, désinformation, obstacle à la concurrence. - Actes terroristes (OIV- SCADA)
Secteur public	Fonctions essentielles : - Maintien de l'ordre. - Approvisionnements essentiels : Eau, alimentation, électricité. - Organisation des secours en cas de sinistre ou de catastrophe. - Gestion de crise - Pour l'Etat, maintien des fonctions régaliennes et des services publics. Intégrité/maitrise/disponibilité du Système d'Information et des données. Vulnérabilités systémiques des Smart-cities, des EPCI	- Blackout électrique. - Attaque de la couche physique : infrastructures, réseaux physiques. - Attaque par déni de service. - Fraude, compromission de processus interne. - Ingénierie sociale. - Diffusion non volontaire ou non maitrisée de données, perte de données. - Externalisation trop poussée ou mal maitrisée, dépendance excessive à l'égard d'un éditeur. - Atteinte à la réputation par les réseaux sociaux ou les médias. - Manipulation, désinformation visant à empêcher ou dégrader l'action de l'Etat ou des collectivités. - Actes terroristes (OIV- SCADA) - Cyber espionnage ou cyber attaques organisés par un état ou sous son contrôle.

La diffusion considérable des réseaux sociaux a rendu possible une très grande variété d'usages qui ont concerné des publics des plus divers. Les libertés de communications et d'associations à grande échelle qu'ils ont permises ont pu être exploitées par des organisations ou des groupes d'influence dont les intentions sont parfois sujettes à caution, voire clairement répréhensibles.

Parmi ceux-là, les auteurs du terrorisme djihadiste ont su exploiter avec une remarquable efficacité les réseaux sociaux, principalement à des fins de propagande et de recrutement. Ce constat qui s'est largement imposé après les attentats de 2015 a principalement mis en eu cause Twitter et Facebook, légitimement accusés d'avoir été les premiers vecteurs de diffusion des djihadistes. Il a abouti à une mobilisation incontestable de ces entreprises et plus généralement des géants du net. La réaction a été une combinaison de technologie et d'analyse humaine destinée à supprimer les contenus terroristes des plateformes dès qu'ils sont signalés et, le cas échéant, à alerter les forces de l'ordre dès qu'apparait un risque imminent pour la sécurité d'une personne. La méthode s'est avérée efficace. Il est beaucoup plus difficile de trouver aujourd'hui des éléments de propagande actifs sur Twitter et Facebook mais l'activité des terroristes sur internet n'a pas disparu pour autant. Elle a simplement changé de support en préférant par exemple l'utilisation de ''Telegram'', un outil de messagerie hébergé dans le cloud et qui peut être chiffré. Ce changement a l'avantage de réduire considérablement l'audience des terroristes, Telegram étant beaucoup moins populaire que Facebook ou Twitter, mais il a aussi l'inconvénient de ne plus permettre aux services de sécurité de pister les réseaux ce qui était possible auparavant sur les deux grands réseaux sociaux.

L'autre grand motif de reproche fait aux réseaux sociaux grand public concerne l'influence qu'ils ont pu avoir sur le déroulement de certaines élections, en particulier aux Etats-Unis à l'occasion du dernier suffrage présidentiel ou lors du référendum sur le Brexit. Les accusations ne concernent pas seulement la diffusion de fausses informations ''fake news'' ou de messages à caractère haineux ou racistes, ils visent également la transmission automatisée et ciblée d'informations et d'avis auxquels l'utilisateur adhère déjà. Les algorithmes qui en sont à l'origine permettent en effet d'en adapter le contenu aux gouts et opinions des membres du réseau en réduisant ainsi leur potentiel d'esprit critique. Autre sujet de préoccupation, l'image que donnent les réseaux sociaux de l'état de l'opinion qui peut créer une distorsion dans la perception qu'ont les politiques de l'avis du public. Certains utilisateurs s'expriment davantage que d'autres et se rendent ainsi plus visibles, ce qui peut amener les élus à surestimer leur poids dans la population. Enfin, la preuve est faite que l'opinion et également les représentants politiques peuvent être manipulés par des dispositifs automatisés, les ''usines à trolls'' générateurs d'avis et de messages politiquement orientés et massivement diffusés.

Le risque pour le bon fonctionnement des processus démocratiques est avéré et reconnu par les dirigeants de Facebook, principalement concerné mais qui semble bien décidé à le réduire. Pour autant, les méthodes pour y parvenir ne paraissent pas évidentes ainsi que le constatent les mêmes responsables. La mise au point d'algorithmes spécifiques destinés à corriger ces problèmes ou l'intervention de modérateurs humains n'offrent qu'une protection insuffisante et interrogent sur les risques d'une censure peu compatible avec la liberté d'expression.

Il parait clair que les moyens engagés par ces réseaux ne pourront se substituer à ce qui apparait aujourd'hui indispensable mais difficile à mettre en œuvre : un renforcement substantiel de la pédagogie des usages de ces réseaux afin de réduire les risques et dérives qu'ils peuvent provoquer. Un tel enseignement devrait concerner en particulier les enfants et les adolescents car ceux sont eux qui paraissent les plus exposées, à plus d'un titre.

Une enquête présentée par le Ministère de l'Education pointe les effets négatifs sur le temps de sommeil des jeunes lié un usage excessif et souvent nocturne. Près de 23 % des 11-14 ans peuvent rester éveillés ou se réveillent pour aller sur Internet la nuit. Chez les 15-18 ans, c'est le cas d'environ 40% d'entre eux.

La question des effets nocifs des réseaux sociaux sur la santé mentale des jeunes paraît préoccupante. L'Organisation Mondiale de la Santé est en passe de reconnaître le "trouble du jeu vidéo" (Gaming disorder) comme une pathologie du registre de l'addiction. Ce classement est l'aboutissement d'un constat planétaire mais qui ne fait cependant pas l'unanimité en raison du déficit d'étude épidémiologique susceptible d'apporter une confirmation scientifique définitive. Le ministère de la Santé américain constate par ailleurs que le taux de dépression des adolescents et jeunes adultes s'est accru de 60 % en seulement six ans et nombreux sont les psychiatres qui pointent les corrélations entre abus d'écrans, anxiété et dépression. Là encore, outre Atlantique les études scientifiques font défaut. Les chercheurs britanniques de la Royal Society for Public Health (RSPH) sont beaucoup plus catégoriques et incriminent Instagram, Facebook, Twitter et Snapchat dont les usages constitueraient une atteinte au bien-être et à la santé mentale de leurs jeunes utilisateurs, avec un effet particulièrement nocif pour Instagram. Effet secondaire non négligeable lié à une durée moyenne d'utilisation quotidienne des écrans d'environ 3h30 chez les 15-24 ans en France, la baisse d'activité physique consécutive contribue à réduire d'autant plus la durée de vie des utilisateurs qu'elle peut se conjuguer avec des troubles mentaux.

Parmi les effets négatifs des réseaux sociaux, le Ministère de l'Education pointe également la fréquence des cas de cyberviolence qui concernent 14 % des élèves en école primaire et près de 20 % des collégiens, et de cyberharcèlement produit par la répétition intentionnelle d'une ou plusieurs formes de cyberviolence, dans la durée.

Compte tenu de l'importance des risques qu'ils présentent pour les jeunes, l'usage des réseaux sociaux est devenu un enjeu prioritaire pour le ministère de l'Education et la communauté éducative depuis plusieurs années.

Ces dernières années ont donc vu la multiplication des risques liés aux usages des réseaux sociaux dans des domaines très différents qu'ils soient politiques, sociaux ou liés à la sécurité ou la santé. Tous ont cependant en commun de constituer des menaces qui peuvent être d'un niveau élevé pour les secteurs concernés mais dans la plupart des cas, l'évaluation scientifique des causes et des impacts est pénalisée par la nouveauté du phénomène ainsi que l'évolutivité des usages et l'innovation régulière qui les caractérise. Les dispositifs techniques ou humains destinés à réduire ces risques resteront certainement longtemps exploratoires avant de parvenir à une maturité suffisante pour en garantir la maîtrise.

Aller au sommaire

Le comité de la filière industrielle de sécurité (CoFIS)

.

Il est constitué de membres de droit et de trois collèges :

Les membres de droit du comité sont :

• le Premier ministre et les différents ministres concernés (en particulier justice, économie et des finances, affaires sociales et santé, intérieur, affaires étrangères, environnement, défense, enseignement supérieur, agriculture) ;

• le commissaire général aux investissements ;

• le directeur général de la banque publique d'investissement.

Participent également aux délibérations du comité : le Secrétaire général de la défense et de la sécurité nationale (SGDSN), le Directeur général des entreprises (DGE)), le délégué interministériel à l'intelligence économique (D2IE), et le délégué ministériel aux industries de sécurité (DMIS).

Les trois collèges, renouvelés tous les trois ans, sont composés de la façon suivante :

• le collège des opérateurs et utilisateurs non étatiques (représentants des associations et collectivités territoriales, acteurs de la sécurité, représentants des opérateurs d'importance vitale publics et privés.

• le collège des industriels (représentants d'entreprises adhérentes au conseil des industries de confiance et de sécurité (CICS) et représentants des pôles de compétitivité et de clusters régionaux d'industriels.

• le collège des personnalités qualifiées désignées par les pouvoirs publics (parlementaires, représentants du monde de la recherche publique et privée, d'instances ou organismes impliqués dans les volets juridique, normatif et organisationnel de la sécurité.

Le conseil des industries de la confiance et de la sécurité (CICS)

Il a été créé par les industriels de la sécurité pour procurer un interlocuteur industriel aux pouvoirs publics dans le cadre de la filière industrielle de sécurité avec l'ambition de contribuer à la promotion, en France et à l'exportation, de nouveaux programmes servant de support au développement de compétences et d'emplois.

Présentation

La filière des industriels de sécurité regroupe les entreprises apportant des services, solutions et technologies qui permettent de protéger l'Etat, la société, l'économie, les citoyens contre les actions hostiles ou les risques naturels. Le Conseil des industriels de la confiance et de la sécurité a pour vocation de fédérer l'ensemble des industriels de la filière sécurité en France.

Les priorités du CICS

Le CICS est animé par trois priorités :

- se doter d'une connaissance de l'évolution des besoins capacitaires à moyen terme

- consolider une vision partagée de la politique industrielle à mettre en oeuvre, en France et en Europe, pour développer le contenu technologique de la filière, conquérir des marchés exports et protéger les domaines de souveraineté

- concentrer les moyens financiers, publics et privés, nationaux et européens, sur des actions de R&D et surtout sur des démonstrateurs qui constituent une étape indispensable pour proposer aux opérateurs de nouvelles solutions innovantes

Aller au sommaire

❑ Synthèse

La cyber-sécurité est un sujet de formation depuis de nombreuses années ; des programmes solides existent et font référence dans ce domaine. Ainsi, la formation ESSI de l'ANSSI existe depuis une vingtaine d'années, même si elle a subi de nombreuses transformations durant cette période. La spécialisation en Sécurité des Systèmes et des Réseaux de Télécom SudParis existe depuis plus de 12 ans, dans sa version intégrée au programme ingénieur et sous forme de Mastère Spécialisé. Un vivier significatif d'étudiants a donc pu être formé ces dernières années.

Les différents mécanismes de labellisation et de coopération avec l'ANSSI permettent de valider à la fois la pertinence et la qualité des formations. Le programme CyberEdu fournit à toute formation aux domaines du numérique des outils pour intégrer la cyber-sécurité dans le programme de formation. La labellisation SecNumedu valide pour les étudiants et les entreprises le fait qu'une formation, au niveau M2, est conforme au référentiel de compétences et de métiers cyber-sécurité.

Le bon fonctionnement d'une formation repose également sur une équipe de recherche solide, dont l'activité permet d'assurer une bonne visibilité à la formation. Cela permet d'assurer un vivier de stages, dont certains à l'étranger, d'obtenir des sujets de projets, et de maintenir un vivier de vacataires professionnels du domaine de la cyber-sécurité pour animer nos formations.

❑ Difficultés

Le marché de l'emploi dans le domaine de la sécurité est tendu. Il va le rester dans les années à venir, en raison du déficit très important actuellement dans ces métiers, alors que la pénétration du numérique dans tous les secteurs d'activité va accroitre le besoin. De plus, la LPM impose aux OIV de sécuriser leurs infrastructures numériques. Le marché des services autour de la conformité, de la détection et de la réponse aux incidents de cyber-sécurité va donc continuer de croitre. Nous notons par exemple en ce moment une tension importante autour des métiers du Security Operating Center en Ile de France et dans la région de Toulouse. La mise en place au niveau ECSO de la task-force EHR4CYBER (ressources humaines pour la cyber-sécurité), ainsi que les activités de l'ENISA répertorient ces difficultés au niveau Européen.

L'évolution des services numériques est extrêmement rapide. Par conséquent, se maintenir au niveau tant des services que des risques numériques demande une politique de formation continue qui prenne en compte les services émergeants et propose des formations adaptées à ces services. Les enjeux aujourd'hui incluent donc à la fois la mise à niveau de systèmes « historiques » et la sécurisation « par défaut » des nouveaux services.

De nouveaux métiers pour lesquels la cyber-sécurité sera importante vont également émerger autour du transport (véhicules autonomes en particulier), de la ville intelligente, de l'énergie. Pour ces nouveaux métiers, nous ne disposons pas encore d'équipes, ni de plates-formes pour monter des programmes d'enseignement.

❑ Quelques pistes de progrès

Le niveau du besoin en formation en cyber-sécurité, tant formation initiale que formation professionnelle tout au long de la vie, va continuer à s'accroitre pendant encore plusieurs années. Pour combler le retard pris, il faudrait donc en particulier :

1. Accroître les capacités des formations de référence pour disposer de pôles d'excellence reconnus et attractifs au niveau mondial pour être toujours à l'état de l'art dans un domaine particulièrement innovant.

Ces pôles d'excellence pourraient par exemple se construire autour des formations opérées par IMT Atlantique en Bretagne, Eurecom en région PACA, l'ENSHEEIT dans le sud-ouest ou Télécom SudParis en région parisienne ; tous ces pôles disposent du vivier industriel et scientifique nécessaire à leur développement.

2. Développer les plates-formes d'expérimentation.

Le développement des cyber-ranges et autres formes d'exercices et d'ateliers semble une priorité absolue tant pour la formation initiale que pour la formation continue.

Il serait en outre souhaitable que certaines de ces cyber-ranges se positionnent sur des secteurs spécifiques, par exemple l'industrie du futur/usine 4.0 (Internet Industriel, protocoles, …) ou le véhicule connecté, avec les investissements matériels et techniques appropriés, ainsi qu'une activité de recherche et d'innovation dans ces domaines pour en comprendre le fonctionnement, les risques et les solutions pour s'en prémunir.

3. Accroitre le vivier d'étudiants susceptibles de suivre des formations en cyber-sécurité et de devenir des professionnels du domaine.

Pour développer le vivier ingénieur, il serait souhaitable que tous les étudiants désireux de se former dans le domaine de la cyber-sécurité puissent avoir accès à des formations d'autres écoles sur le sujet.

Il est également nécessaire de développer des formations à Bac+3 en cyber-sécurité, notamment en ce qui concerne l'opérationnel (SOC, détection de premier niveau, gestion des opérations, …).

4. En complément de la certification des formations, il serait utile de développer des mécanismes de certification des étudiants, ou des compétences.

Les certifications professionnelles actuelles demandent plusieurs années d'exercice professionnel avant d'être accessibles. Il est donc difficile pour un employeur de juger du niveau technique des étudiants recrutés.

Une meilleure accessibilité aux certifications orientées compétences (que peuvent par exemple représenter PASSI, PRIS et PDIS) pourrait prendre la forme d'une certification « junior » de celles-ci.

5. Faire monter en compétence les étudiants suivant des filières numériques

La mise en place de CyberEdu est une première étape. Il serait utile de développer quelques modules plus focalisés sur le développement et sur l'administration de systèmes.

Aller au sommaire

L ’approche CRR du CERT-US

Le Cyber Resilience Review (CRR) est une méthode d'évaluation mise au point par le Department of Homeland Security (DHS) des États-Unis. Il s'agit d'un examen volontaire de la résilience opérationnelle et des pratiques de cybersécurité mis au point par le DHS pour les entreprises, les opérateurs des infrastructures critiques et les structures publiques d’Etat et territoriales. Le CRR a une approche orientée services, l'un des principes fondamentaux du CRR est qu'une organisation déploie ses ressources (personnes, informations, technologies et installations) pour soutenir des missions opérationnelles spécifiques (ou services). Il est disponible en téléchargement libre sur le site Web de DHS.

https://www.us-cert.gov/ccubedvp/assessments

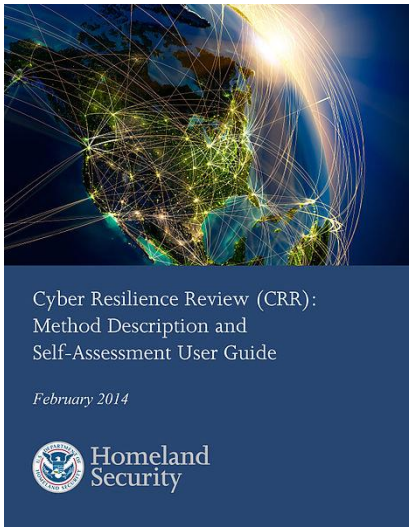
Il peut être utilisé pour une auto-évaluation ou comme cadre de référence d’une évaluation confiée à un prestataire extérieur. Les outils disponibles comprennent un outil automatisé de saisie (297 questions !) et de génération de rapports, un guide de facilitation, une explication complète (> 500 pages !) de chaque question.

Le DHS s'est associé à la Division CERT du Software Engineering Institute de l'Université Carnegie Mellon pour concevoir et déployer le CRR. Les concepts du CRR sont dérivés du Résilience Management Model (CERT-RMM) élaboré par cette organisation, également disponible en téléchargement

https://cert.org/resilience/products-services/cert-rmm/index.cfm

Le CRR comprend 42 objectifs et 141 pratiques spécifiques extraites du CERT-RMM, organisés en 10 domaines

- Le management des ressources
- Les contrôles
- Le management des configuration
- Le management des vulnérabilités
- Le traitement des incidents
- L management de la continuité de service
- le management des risques
- Le management des dépendances externes
- La formation et sensibilisation
- l’intelligence situationnelle



Aller au sommaire

Aller au sommaire

Ministères, administrations et collectivités locales

	Service	Fonction	Date du rendez vous
Serge JACOB **Vincent STRUBEL**	Premier ministre/SGDSN ANSSI	Directeur-adjoint Protection et sécurité de l'Etat Sous-directeur Expertise	27/04/2017
Guillaume POUPARD	Premier ministre/SGDSN/ANSSI	Directeur général	27/06/2017
Henri VERDIER	Premier ministre/SGMAP/DINSIC	Directeur	13/07/2017
Christophe QUINTIN	Min. de la transition écologique et solidaire/SG	HFDS adjoint	06/04/2017
Marc MORTUREUX	Min. de la transition écologique et solidaire/DGPR	Directeur général	non rencontré
David COMBY	Min. de la transition écologique et solidaire/CGDD	Coordonnateur interministériel délégué pour les programmes GNSS	06/04/2017
Christian DUFOUR	Min. de l'économie et des finances/SG	HFDS adjoint	12/04/2017
Loïc DUFLOT	Min. de l'économie et des finances/DGE/SEN	S/D Réseaux et usages numériques	27/04/2017
Jean-Baptiste CARPENTIER	Min. de l'économie et des finances/DGE/SISSE	Chef de service, Commissaire à l'information stratégique et à la sécurité économique	non rencontré
Jean-Claude MALLET	Min. de la défense	Conseiller spécial du ministre	14/04/2017
Gén. Grégoire BLAIRE	Min. de la défense/Direction interarmées des réseaux d'infrastructure et des systèmes d'information de la défense (DIRISI)	Directeur central	01/06/2017
Jean-Bernard BOBIN	Min. de l'intérieur/DGSCGC / Service de la planification et de la gestion des crises	Chef de service	25/04/2017
Thierry DELVILLE	Min. de l'intérieur/Délégation ministérielle aux industries de sécurité et à la lutte contre les cyber-menaces	Délégué ministériel	22/05/2017
Gén. Bruno POIRIER-COUTANSAIS	Min. de l'intérieur/Service des technologies et des systèmes d'information de la sécurité intérieure	Chef de service	23/05/2017
François MOLINS	Ministère de la justice	Procureur de la République de Paris	11/07/2017
Constant HARDY	Ministère de l'Economie	CCED	18/07/2017
Marc MEUNIER	Préfecture de police de Paris	Préfet, secrétaire général de Zone de défense et de sécurité de Paris	11/05/2017
Sébastien MAIRE	Mairie de Paris	Haut responsable de la résilience	10/05/2017

Aller au sommaire

Etablissements publics, enseignants et chercheurs

	Etablissement	Fonction	Date du rendez vous
Gilles BREGANT	Agence nationale des fréquences	Directeur général	31/05/2017
Didier ELBAUM et Marc ANDRIES	Banque de France	Contrôleur général-délégation au contrôle sur place	14/06/2017
Jérôme NOTIN	GIP ACYMA (Actions contre la cybermalveillance)	Chef de projet	01/06/2017
Serge ABITEBOUL/Didier REMY	INRIA	Directeurs de recherche	16/05/2017
Hervé DEBAR	Télécom Sud Paris	Professeur, directeur du Dépt. Réseaux et services de télécommunications	19/06/2017
Jean-Max DUTERTRE	Ecole des Mines de Saint-Etienne, Centre microélectronique de Provence	Responsable du département Systèmes et Architectures Sécurisées	15/06/2017
Laurent GILLE	Télécom ParisTech	Professeur	22/05/2017
Arrah-Marie JO	Telecom ParisTech	Doctorante	07/06/2017
Sébastien BOMBAL	EPITA	Responsable de la Majeure Systèmes Réseaux et Sécurité	14/06/2017
Julien NOCETTI	IFRI	Chercheur	30/05/2017

Aller au sommaire

Entreprises et fédérations professionnelles

	Entreprise ou organisation	Fonction	Date du rendez vous
Benjamin GESTIN	Eaux de Paris	Directeur général	07/07/2017
Eric SALOMON	ENEDIS	Directeur régional Paris	07/07/2017
Sylvain CHAPON	ENGIE	Délégué marketing stratégique	06/07/2017
Philippe COTELLE	Airbus	Head of Insurance Risk Management	14/03/2017
Paul THERON	Thales/	Responsable des offres de cyber-défense	26/04/2017
Jean-Noël de GALZAIN	Hexatrust	Président (et président de Wallix)	18/05/2017
Alexis CAURETTE	Alliance pour la confiance numérique	Vice-président (et Directeur Global consulting et intégration cybersécurité, Atos)	02/06/2017
Arnaud DUCHAMP	IDnomic	Directeur R&D	24/05/2017
Ahmed BENOUR	AREVA	Directeur SI-nerGIE	20/07/2017
Oliver WILD	VEOLIA	Group Chief Risk Officer	19/07/2017

Aller au sommaire

Aller au sommaire

Bibliographie

date de parution	auteur	titre ou thème	éditeur
050100	Jacques S. Gansler & Hans Binnendijk	Information Assurance: Trends in Vulnerabilities, Threats and Technologies	National Defense University, Washington, D.C.
090000	Franklin D. Kramer, Stuart H. Starr & Larry K. Wentz	Cyberpower and National Security	National Defense University, Washington, D.C.
160200	US department of homeland security	NIST cybersecurity framework (CSF)	Cyberresilience Revue
050000	Jerôme Vicente	Les espaces de la Net-Economie: clusters TIC et aménagement numérique des Territoires	ECONOMICA
070000	Christian Paul	Le défi numérique des Territoires: réinventer l'action publique	AUTREMENT
060300	Hugues de Jouvenel (éditorial) - Anne de Beer (télétravail)	La crise du logement en France - Le télétravail en perspective - Impasse en Tchétchénie	FUTURIBLE
080926	SGDN	Instruction générale interministérielle relative à la sécurité des activités d'importance vitale	
991100	Danielle Bahui-Leyser et Pascal Faure	Nouvelles technologies / Nouvel Etat	La Documentation Française
160706	PM	PacteEtatMetropoles: l'innovation au service des territoires	
120000		Partnering for Cyber Resilience	World Economic Forum
x		International Standards for Management Systems (ISMS)	ISO
150000	Accenture	Making your entreprise cyber resilient	
140000 ?	Symantec	white paper: the cyberresilience blueprint, a new perspective on security	
160000		Le chemin vers la résilience - gestion des cuber-risques	World Energy Council
160627		Face au terrorisme islamiste	GR8 ?
140000	Accenture	Eviter les obstacles: cyber-risque et résilience	
160217	Vincent Roy	Développer la cyber-résilience pour les entreprises	
151217	Maria Lazarte	Des organismes à l'abri des cyber-attaques grâce à une boîte à outils de normes sur la sécurité	
160800	Michel Foucher	A quoi servent les frontières	
130000	Alix Desforges	Les frontières du cyber espace	
140428	Alix Desforges	Les représentation du cyberespace : un outil géopolitique	Herodote
121200	Solange Ghernaouti & Christian Aghroum	Cyber-résilience, risques et dépendances: pour une nouvelle approche de la cyber-sécurité	CAIRN info
160700	Philippe Cotelle, Philippe Wolf & Benedict Suzan	La maîtrise du risque cyber sur l'ensemble de sa chaîne de valeur et son transfert vers l'assurance	IRT SYSTEM X

Aller au sommaire

Bibliographie (suite)

150420	René-François Bernard, Ilarion Pavel & Henri Serres	Cyberassurance Rapport CGE	CGE + benchmark Trésor
170000	Simon Leguil, Nicolas Grorod, Gaspard Ferey	Les risques cyber, mirage ou tendance de fond pour l'assurance ?	Mines ParisTech
170100	Gabrielle Desarnaud	Cyberattaques et systèmes énergétiques	IFRI
160100	Gabrielle Desarnaud	Cyberattaques et systèmes énergétiques	IFRI
170126	Isabelle Roux-Trescaze	Contribution des organismes contrôlés par le CGeFi à la politique d'open data	CGeFi
160706		Pacte Etat Métropoles	
170100	Gabrielle DESARNAUD	Cyberattaques et systèmes énergétiques	Etudes de l'IFRI
140512	Thomas Petermann, Harald Bradke, Arne Lüllmann, Maik Poetzsch, Ulrich Riehm	Que se passe-t-il pendant un blackout?	Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) Karlruher Institut für Technologie (KIT)
151100	the scottish government	Safe, secure and prosperous - a cyber resilience strategy for Scotland	APS group scotland
170217	Lélia de Matharel	Les 12 secteurs d'activité que le machine learning va faire exploser	JND (journal du net)
170300	Rand Hindi (CNN) et Lionel Janin (France Stratégie)	Anticiper les impacts économiques et sociaux de l'intelligence artificielle	France Stratégie
170326	Clément Bertholet et Laura Létourneau	Ubérisons l'Etat	Armand Colin
170400	Emilie Bourdu, Thierry Weil	Numérique et emploi, quel bilan?	La Fabrique de l'Industrie
170117	Sandra Pfeiffer	How can organisations deal with systemic risks	IRGC
160600	Alexandar Javanovic	EU project smart resilience	Research Gate
		Ransomware	Ivanti
150915	Alain Bonneau	cybersécurité vs cyberrésilience	COBIT
170300	Assia TRIA et Jacques FOURNIER	Scuriser l'internet des objets	Industrie & technologies n°996
160000		The road to resilience: managing cyber risks	World Energy Council
110000	Laurie J Van Leuven	water/wastewater infrastructure security: threats and vulnerabilities	Springer
170200	Philippe Wolf	internet of every things et sécurité	L'énergie et les Données
170207	Nathalie Nevejans	Traité de droit et d'éthique de la robotique civile	LEH éditions
160000	OSCP	Rapport annuel 2015 OSCP	www.observatoire-cartes.fr
170123	Eric A.Caprioli	Attaques DDoS, le cas d'EDF et ses conséquences juridiques	Les experts du numérique
161114	Vincent Bazillio	Les 5 commandements de la cybersécurité en entreprise	Axians

Aller au sommaire

Bibliographie (suite)

170510		Les constructeurs automobiles face à la cybersécurité	Usine nouvelle
150000	Cécile Wendling	Entreprises et cybersécurité à l'horizon 2020	Futuribles international
170200	Nathalie Nevejans	Responsabilité des robots : "Appliquons nos règles de droit !"	Le.Point.fr
080926		instruction générale 6600 relative à la sécurité des secteurs d'importance vitale	
170408		why every thing is hackable	Science and technology
170201	Cécile Desjardins	Cyberattaques, catastrophes, réputation : l'ère de l'aléatoire	Les Echos
170500		Comment l'équipe de Macron s'était préparée au piratage	Rédaction JDD
170515		WANNAcry	
170100	Nathalie NEVEJANS	Traité de droit et d'éthique de la robotique civile	LEH éditions
160920	Lloyd's	Cyber survey report	
170522	Symantec	Récupérer d'une attaque de virus en 5 étapes	symantec.com
170400	Laurent Gille	Quel avenir pour les communications électroniques	
2016	Trend micro	Trend micro security prediction for 2017	
170531	Tanguy de Koatpont	Les entreprises françaises face à l'explosion de la cybercriminalité	blog Euler Hermès
170531		La cyberfraude, phénomène en expansion	blog Euler Hermès
170113		Pathway into cybercrime	National Crime Agency (NCA)
170600	Arrah-Marie JO	Economie de la sécurité de l'information	Thèse Telecom ParisTech
170100	Thierry Delville, Eric Freyssinet…	Etat de la menace liée au numérique en 2017	Ministère de l'intérieur - DMISC
170100		Livre blanc Cybersécurité et confiance numérique	Hexatrust - Systematic Paris Région
170200		Etude annuelle sur la cyber résilience en France	Ponemon Institute
170400	Verizon	2017 Data Breach Investigations Report	VerizonEnterprise.com
170000		The defender's dilemna	rapport de la RAND
170411		G7 Declaration on Responsible States Behavior in Cyberspace	
160900	Gregory Albertyn, etc…	Gouverner à l'ère du numérique	CESIN & Solutions numériques
		Towards a new intiative for cyber insurance	Digimutual

Aller au sommaire

Bibliographie (suite)

161200	Infineon, NXP, STMicroelectronics, ENISA	Common position on cybersecurity	
170000	John S. Davis II, Benjamin Adam Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, Michael Chase	Stateless attribution : Toward international accountability in Cyberspace	Rand Corporation
170000	Young Health Movement	#StatusOfMind Social media and young people's mental health and wellbeing	Royal Society For Public Health (UK)
170000	Simon Leguil, Nicolas Grorod, Gaspar Ferey	Les risques cyber, mirage ou tendance de fond pour l'assurance	mémoire Mines ParisTech
160705		Strengthening Europ's Resilience System	Union européenne
170200		Etude annuelle sur la cyber-résilience	Ponemon
170200	Poupard, Coustillère, Berthier, Wattin-Augouard,	Recueil d'articles sous le titre : "Cyber guerre" L'heure de l'action	Revue Défense et Sécurité Internationale
170200	DEFENSE SCIENCE BOARD	Task force on cyber deterrence	Department of Defense (DoD)
170613		Cyberespionnage via les APT	docaufutur
170619		L'UE répondra aux cyber attaques	Le FIGARO
170620	Jacques Henno	L'IA entre dans l'arsenal de la cybersécurité	Les ECHOS
130901	Ann Cavoukian, Mark Dixon	Privacy and Security by Design : An Entreprise Architecture Approach	Commissariat à l'information et la protectiopn de la vie privée du Canada https://www.ipc.on.ca/?redirect=https://www.ipc.on.ca/&lang=fr
161215	CIGREF	Le cyber Risque dans la gouvernance de l'entreprise	CIGREF
170627	Nicolas Brouste Florian Pierrat	Une cyberattaque mondiale frappe des entreprises et des administrations	Le Figaro
170000	ANSSI	2017-2022 : 5 ans pour la transformation numérique de la France	
170706	Louis Adam	L'ONU fait le point sur la cybersécurité à l'échelle mondiale	
170000		Emerging riscks report 2017	LLOYD's
170000		Rapport risques émergents 2017	LLOYD's
170000	Gaspard Ferrey, Nicolas Grorod, Simon Leguil	L'assurance des risques cyber	TelecomParisTech, MinesParisTech
170000	Philippe Muller Feuga	Cyber-espace, nouvelles menaces, nouvelles vulnérabilités	Sécurité Globale / n°9 éditions ESKA
170000	Samantha Bradshaw, Philip N.Howard	Troops, trolls and Troublemakers	University of Oxford
170718	Didier Barathon	Les stratégies de cyber-sécurité en retard par rapport aux attaques attaques	451 research et Thalès
170805	Stanislas de Maupéou	La cyber-sécurité, clef de notre liberté numérique	Les Echos
170306	Anne-Yvonne Le Dain	L'évaluation de la stratégie nationale de recherche en énergie	Assemblée Nationale
120600	ANSSI	Maîtriser la SSI pour les systèmes industriels	

Aller au sommaire

Bibliographie (suite)

150109	Damien Bancal	Le groupe anonghost lance une opération contre la France	Zataz.com
170000		Cyber-crime in West Africa	interpol et trend micro
170113		’Pathways into cyber crime	National Crime Agency/National Cyber Crime Unit/Prevent Team
160000		’Le web underground en France : sous le sceau de la vigilance’’	Trend micro
150800	Daniel Ventre	’La cyberguerre des gangs aura-t-elle lieu ?’’	IFRI
140100	Bob Kolasky	The CIP report	DHS
130400	Argone national laboratory	Resilience mesurement index	US department of energy
130702	Chris Zebrowski	The nature of resilience	journal "resilience"
170700	Daniel Guinier	Cyber attaques et Macronleaks / diffusion de fausses informations	Doctrine
140717		PSSIE	ANSSI
170923		Schumpeter big tech big trouble	The economist
160500	INSEE	Sécurité numérique et médias sociaux dans les entreprises en 2015	INSEE Première n°1594
170000	Accenture	Cost of cyber crime study	PONEMON
171017	Jean-Philippe Bichard	lancement national de la plateforme ACYMA	Cyber risk news
150817	Philippe Woloszyn	Inductive Modelling of Vulnerable Sustainability Systems	Scientific research publishing
160926		Security framework	Industrial internet consortium
171024		Cybersécurité 2.0 : suivi de la réunion du Conseil européen et du sommet numérique de Tallinn	SGAE
170800		securing cyber assets	NIAC
170000	Olivier Levillain, Pascal Chour	La sécurité du numérique dans l'enseignement supérieur	ANSSI
170000	Yann Verdo	Cybersécurité : la science est entrée en guerre	
161103	Julien Bedhouche	Response to the European Commission consultation on the public-private partnership on cybersecurity and possible accompanying measures	FERMA
170513	G7	communiqué	

Aller au sommaire

Aller au sommaire

Sigles et glossaire

ACN	Alliance pour la Confiance Numérique – Association d'entreprises
ACPR	Autorité de contrôle prudentiel et de résolution - Institution chargée de la surveillance de l'activité des banques et des assurances en France.
ACYMA	Dispositif gouvernemental contre la cybermalveillance mettant en œuvre la plateforme www.cybermalveillance.gouv.fr d'assistance aux victimes.
APT	Advanced Persistent Threat. Type de piratage informatique évolué, furtif et continu ciblant une entité spécifique pour des durées prolongées et le plus souvent à des fins d'espionnage.
ANFR	Agence Nationale des Fréquences
ANR	Agence Nationale de la Recherche
ANSSI	Agence nationale de la sécurité des systèmes d'information
APT 28	Advanced Persistent Threat (APT) également nommée ''Cosy Bear'' et probablement d'origine russe.
APT 29	Advanced Persistent Threat (APT) également nommée ''Fancy Bear'' et probablement d'origine russe.
BCE	Banque Centrale Européenne
Botnet	Réseaux de programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches. Il s'agit le plus souvent de réseaux de machines zombies, utilisés pour des usages malveillants, comme l'envoi de spam et virus informatiques, ou les attaques informatiques par déni de service (DDoS).
BYOD	Abréviation de l'anglais « bring your own device » (« apportez vos appareils personnels »). C'est une pratique qui consiste à utiliser ses équipements personnels (smartphone, ordinateur portable, tablette électronique) dans un contexte professionnel.
CAPIC	Centres d'analyse et de partage de l'information en cybersécurité. Equivalent français des ISAC mis en place aux Etats-Unis.
CCED	Commissariat aux communications électroniques de défense.
CERT - CSIRT	Computer emergency response team (CERT) ou computer security incident response team (CSIRT) - Centre d'alerte et de réaction aux attaques informatiques destiné aux entreprises ou aux administrations.
CGDD	Commissariat général au développement durable.

Aller au sommaire

Sigles et glossaire

CHAI	Comité d'harmonisation de l'audit interne de l'État.
CICS	Conseil des Industries de la Confiance et de la Sécurité
Cloud	Consiste à exploiter la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'Internet.
COFIS	Comité de filière des industries de sécurité
CoFIS	Comité de la Filière Industrielle de la Sécurité
CRR	Cyber Resilience Review est une méthode d'évaluation mise au point par le ministère de la sécurité intérieure (Department of Homeland Security - DHS) des États-Unis.
CyberEdu	Démarche lancée par l'ANSSI afin d'introduire les notions de cybersécurité dans l'ensemble des formations en informatique de France. Les formations en question reçoivent le label CyberEdu.
DAJ	Direction des Affaires Juridiques
Dark web	Contenu du World Wide Web qui existe sur les darknets qui utilisent l'internet public mais sont seulement accessibles via des moyens spécifiques.
DDoS	Distributed Denial of Service – Type d'attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser.
DGAFP	Direction Générale de l'Administration et de la Fonction Publique
DGE	Direction Générale des Entreprises du Ministère de l'Economie et des Finances
DGSCGC	Direction générale de sécurité civile et de la gestion des crises du Ministère de l'Intérieur
DGSIP	Direction Générale de l'enseignement Supérieur et de l'Insertion Professionnelle du Ministère de la Recherche et de l'Enseignement Supérieur.
DHS	US Department for Homeland Security – Ministère de la sécurité intérieure des USA
DIRISI	Direction interarmées des réseaux d'infrastructure et des systèmes d'information de la défense.
DMIS	Délégué interministériel aux industries de sécurité.
ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information – European Union Agency for Network and Information Security
ENS	Ecole Normale Supérieure

Sigles et glossaire

ENTSOE	European Network of Transmission System Operators for Electricity. Association représentant 41 gestionnaires de réseau de transport d'électricité de 34 pays à travers l'Europe.
ESN	Entreprise de services du numérique
ESSI	Expert en Sécurité des Systèmes d'Information – Titre décerné à des agents de l'Etat ayant suivi une formation longue réalisée par l'ANSSI.
EternalBlue	Logiciel développé par la NSA pour exploiter une faille de sécurité existante sur le système Windows XP. A permis le développement des rançongiciels Wannacry et NotPetya.
Faille ''zero-day''	Vulnérabilité informatique n'ayant fait l'objet d'aucune publication, n'ayant aucun correctif connu et ne faisant l'objet d'aucune protection.
FERMA	Federation of European Risk Management Associations – Fédération européenne des professions de management du risque
FSSI	Fonctionnaire de la sécurité des systèmes d'information, placé auprès du Haut Fonctionnaire de Défense et de Sécurité (HFDS) dans chaque ministère.
FUI	Fonds unique interministériel - Programme destiné à soutenir la recherche appliquée pour aider au développement de nouveaux produits.
HAND	Hackers Against Natural Disasters. Association dont l'objectif est de préparer aux catastrophes naturelles, afin de réduire le nombre de victimes. Voir : http://hand.team
Hexatrust	Association d'entreprises du secteur de la sécurité des systèmes d'information et de la cybersécurité.
HFDS	Haut fonctionnaire de défense et de sécurité
HOT	Humanitarian OpenStreetMap Team. Organisation internationale à but non lucratif développant des cartes gratuites au profit des organisations de secours en cas de crises. www.hotosm.org
IFRI	Institut français des relations internationales
IMT	Institut Mines-Télécom
INRIA	Institut national de recherche en informatique et en automatique
IoT	Internet des objets (Internet of Things), extension d'Internet au mondes des objets connectés.
IRT SYTEM X	Institut de Recherche Technologique mis en place dans le but de soutenir l'innovation en France en 2012 dans le domaine de l'ingénierie numérique des systèmes du futur.

Aller au sommaire

Sigles et glossaire

ISAC	Information Sharing and Analysis Centers - Modèle d'origine américaine d'organisation à but non lucratif regroupant des membres publics et privés destinée à centraliser et partager l'information sur les menaces d'origine cyber.
LPM	Loi de programmation militaire.
Malware	Logiciel malveillant développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté.
MCO	Maintien en condition opérationnelle - Ensemble des mesures prises pour garantir que la bascule vers un environnement dégradé n'entraîne pas une altération inacceptable des conditions de travail habituelles.
MIRAI	Logiciel malveillant qui transforme des objets connectés utilisant le système d'exploitation Linux en bots contrôlés à distance pour réaliser des attaques à grande échelle sur les réseaux.
MOA	Maîtrise d'ouvrage
NotPetya	Logiciel malveillant destructeur de données apparu en juin 2017
NotPetya	Logiciel malveillant qui apparait sous la forme d'un rançongiciel mais qui est en fait un destructeur de données (wiper). Apparu en Ukraine en juin 2017.
NSA	National Security Agency : Agence de renseignement d'origine électromagnétique et de la sécurité des systèmes d'information et de traitement des données du gouvernement américain.
NSCR	Niveau synthétique de cyber résilience évalué à partir des référentiels d'évaluation de la cyber-résilience
OIV	Opérateurs d'importance vitale - Organisation identifiée par l'État comme ayant des activités indispensables ou dangereuses pour la population.
OSM	Open Street Map www.openstreetmap.org est un projet qui a pour but de constituer une base de données géographiques du monde permettant de créer des cartes en licence libre.
PAP	Projet annuel de performance. Les PAP sont annexés au projet de loi de finances
PCA	Plan de continuité de l'activité
Petya	Logiciel malveillant de type rançongiciel (ransomware) apparu pour la première fois en mars 2016 en Ukraine.

Aller au sommaire

Sigles et glossaire

Piranet	Plan gouvernemental complément de Vigipirate en cas d'attaque sur les systèmes d'informations.
PRA	Plan de reprise de l'activité
Privacy by design	La protection de la vie privée dès la conception correspond à un ensemble de dispositions mises en œuvre tout au long du développement d'un système pour protéger les données personnelles qu'il utilisera ou stockera.
PSSIE	Politique de Sécurité des Systèmes d'Information de l'Etat
Ransomware	Ou rançongiciel. Logiciel malveillant qui prend en otage des données et exige une rançon pour les restituer à leur propriétaire.
RAP	Rapport annuel de performance. Présente les résultats des administrations au regard des engagements pris en loi de finances
RAPID	Régime d'appui à l'innovation duale - Dispositif de soutien des projets de recherche industrielle présentant des applications militaires mais aussi des retombées pour les marchés civils.
RGPD	Règlement général sur la protection des données (en anglais : General Data Protection Regulation, GDPR)
RSSI	Responsable de la sécurité des systèmes d'information qui garantit la sécurité, la disponibilité et l'intégrité du système d'information et des données d'une organisation.
SCADA	Système d'acquisition et de contrôle de données (Supervisory Control And Data Acquisition) est un système de télégestion à grande échelle permettant de contrôler à distance des installations techniques.
SecNumedu	Label attribué par l'ANSSI aux formations initiales en cybersécurité de l'enseignement supérieur en France selon des critères définis par l'Agence.
Security by design	La sécurité dès la conception correspond à un ensemble de dispositions mises en œuvre tout au long du développement de logiciels ou de matériels afin de les rendre exempts de vulnérabilités et résistants aux attaques.
SG	Secrétaire Général ou Secrétariat Général d'un ministère.
SGDSN	Secrétariat général de la Défense et de la Sécurité nationale

Aller au sommaire

Sigles et glossaire

Shadow Brokers	Groupe de hackers connu pour avoir dévoilé en 2016 des outils d'espionnages, entre autres, de l'Equation Group, une unité de hackers soupçonnée d'être lié à la National Security Agency (NSA).
Shamoon	Virus informatique utilisé en 2012 contre la compagnie pétrolière saoudienne Saudi Aramco pour détruire son réseau informatique.
Stuxnet	Ver informatique découvert en 2010 qui aurait été conçu pour s'attaquer aux centrifugeuses d'enrichissement d'uranium du programme nucléaire iranien.
Titan Rain	Advanced Persistent Threat (APT) qui a visé des entreprises ou des institutions américaines durant plusieurs années à partir de 2003.
VISOV	Volontaires Internationaux en Soutien Opérationnel Virtuel. A ssociation regroupant une communauté virtuelle francophone de volontaires numériques en gestion d'urgence pour contribuer à la sécurité civile. Voir : http://www.visov.org/
Wannacry	Logiciel malveillant de type rançongiciel auto-répliquant. Utilisé en mai 2017 lors d'une cyberattaque mondiale touchant plus de 300 000 ordinateurs dans plus de 150 pays
WIFI	Appellation d'un réseau permettant de relier par ondes radio plusieurs appareils informatiques (ordinateur, routeur, smartphone, modem Internet, etc.)