Lettre d'information économique

Sommaire

Décembre 2020

Editorial

En cette année 2020, marquée par les effets d'une crise sanitaire sans précédent, l'ensemble de la DRSD a adapté et poursuivi sans interruption sa mission de contre ingérence dans le domaine économique, tant dans l'accompagnement de la protection des biens stratégiques, que dans le conseil en termes d'anticipation face aux risques et menaces constatés.

Dans un contexte de guerre économique de plus en plus assumée par certains Etats, la mise en place de dispositifs normatifs à vocation concurrentielle est de plus en plus manifeste comme l'illustre la mise en place du crédit social chinois.

Par ailleurs, s'ajoute à cette conjoncture sécuritaire dégradée, des menaces terroristes et criminelles persistantes, opportunistes et toujours plus sophistiquées.

Aussi, la DRSD, au plus près des sujets de préoccupation de l'ensemble des acteurs économiques, poursuit-elle ses prestations de sensibilisation adaptée aux besoins de chaque organisme et entreprise, pour leur permettre d'adopter une posture de vigilance et d'anticipation permanente.

Au seuil de cette nouvelle année, dans un contexte économique particulièrement difficile, je vous adresse mes vœux les plus chaleureux pour 2021.
Soyez assurés que la DRSD continuera inlassablement à vous accompagner au plus près et à vous protéger des menaces qui touchent l'ensemble des acteurs économiques de la sphère Défense.

Vous pouvez compter sur nous !

Général de Corps d'Armée Eric Bucquet
Directeur du Renseignement et de la Sécurité de la Défense

Les prestations de sensibilisation aux besoins des entreprises

L'environnement économique se caractérise par une accélération des changements liés à un contexte concurrentiel toujours plus complexe. Ces changements constituent des opportunités mais peuvent également être sources de risques.

La lutte contre les ingérences étrangères, l'anticipation des tentatives de prédation financière, la détection des atteintes cybernétiques ou encore la protection des informations et des savoir-faire, constituent, plus que jamais des enjeux majeurs auxquels doivent faire face les entreprises : anticiper et réagir de manière appropriée en temps utile sont impératifs.

La mission de contre ingérence économique de la DRSD a pour objectif de prévenir, déceler et neutraliser toute tentative pouvant nuire aux intérêts économiques, financiers, scientifiques et technologiques des entreprises, organismes, centres ou laboratoires liés à la défense.
Dans ce cadre, la DRSD propose aux entreprises des prestations de sensibilisation sur-mesure, à l'adresse de l'ensemble de leurs dirigeants et collaborateurs, à l'aune de leurs objectifs et enjeux spécifiques.

Ces séances ont pour objectif d'augmenter la posture de vigilance et d'anticipation au sein des organisations ainsi que la gestion dynamique des risques engendrés par des ingérences de plus en plus nombreuses et sophistiquées.
Elles représentent également des moments privilégiés, pour dresser un état des lieux pragmatique des menaces constatées, et partager, en toute confiance, sur les problématiques actuelles.

Pour bénéficier d'une sensibilisation adaptée à votre besoin, contactez nous

drsd-cie-sensibilisation.contact.fct@intradef.gouv.fr

Actions de sensibilisation						
COMEX Comités de direction	Responsables, chefs de projets, collaborateurs	Journée entreprise (séminaires annuels)	Sensibilisation généraliste	Sensibilisation thématique	Menaces Numériques - Cybernétiques	Salons

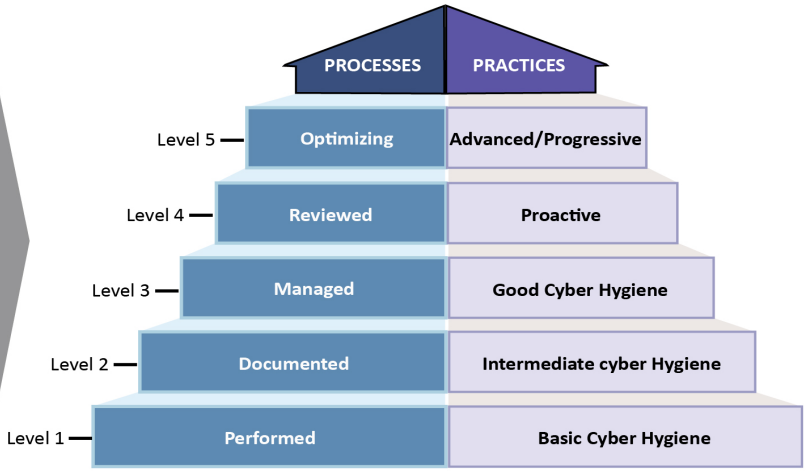
Nouveaux standards de certification du Department of Defense (DoD) américain

En janvier 2020, le *Department of Defense* (DoD) américain a défini de nouveaux standards unifiés de cyber-sécurité (*Cybersecurity Maturity Model Certification* – CMMC). **Ils visent à améliorer la protection des informations sensibles au sein de l'ensemble de la chaîne de valeur des contractants du DoD et deviendront obligatoires pour tous les appels d'offres défense d'ici fin 2021.** Des niveaux de certification de 1 à 5 seront fixés en fonction de la sensibilité du contrat et du niveau d'implication des entreprises et sous-traitants : de CMMC 1 « *Basic Cyber Hygiene* » à CMMC 5 « *Advanced* ».

17 Capability Domains

Access Control (AC)	Incident Response (IR)	Risk Management (RM)
Asset Management (AM)	Maintenance (MA)	Security Assessment (CA)
Awareness and Training (AT)	Media Protection (MP)	Situational Awareness (SA)
Audit and Accountability (AU)	Personnel Security (PS)	System and Communications Protection (SC)
Configuration Management (CM)	Physical Protection (PE)	System and Information Integrity (SI)
Identification and Authentification (IA)	Recovery (RE)	

CMMC Model with 5 levels measures cybersecurity maturity



Cette nouvelle certification s'inscrit dans le cadre des exigences imposées par la réglementation fédérale américaine *Defense Federal Acquisition Regulation Supplement* (DFARS) systématiquement annexée aux contrats au profit de la défense américaine.

.../...

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

Version 1.02 | March 18, 2020

Source : - CYBER SECURITY MATURITY MODEL CERTIFICATION (CMMC) Office of the Under Secretary of Defense / Aquisition and Sustainment / CMMC/
- https://www.acq.osd.mil/cmmc

En conséquence, la mise en conformité à cette certification s'imposera à l'ensemble des industriels de la base industrielle et technologique de défense (BITD) américaine, ainsi qu'à l'ensemble des sous-traitants, américains ou étrangers, s'ils souhaitent remporter des marchés.

A partir du niveau 3 (CMMC 3 « Good Cyber Hygiene »), la mise en conformité impliquera un audit sur pièces et sur place réalisé par un organisme évaluateur tiers qui aura été agrée et certifié par le DoD américain (dit « *CMMC Third Party Assessment Organisation – C3PAO* ») pour délivrer la certification.

CCMC Model : Number of Pratices and Processes introduced at each Level

CMMC Level	Practices	Processes
Level 1	17	-
Level 2	55	2
Level 3	58	1
Level 4	26	1
Level 5	15	1

Les entreprises françaises souhaitant répondre à des appels d'offres ou agissant comme sous-traitants de programmes de défense américains devront obtenir le niveau de certification adéquate, sous peine de se voir refuser la certification et par conséquent perdre des opportunités de marchés.

Cette nouvelle certification imposant la mise en place d'un audit de conformité supplémentaire engendrera des risques potentiels de perte, de fuite ou de captation d'informations stratégiques si les conditions de protection et de sécurité d'accès aux systèmes d'Informations ne sont pas réunies.

Des pratiques cumulatives

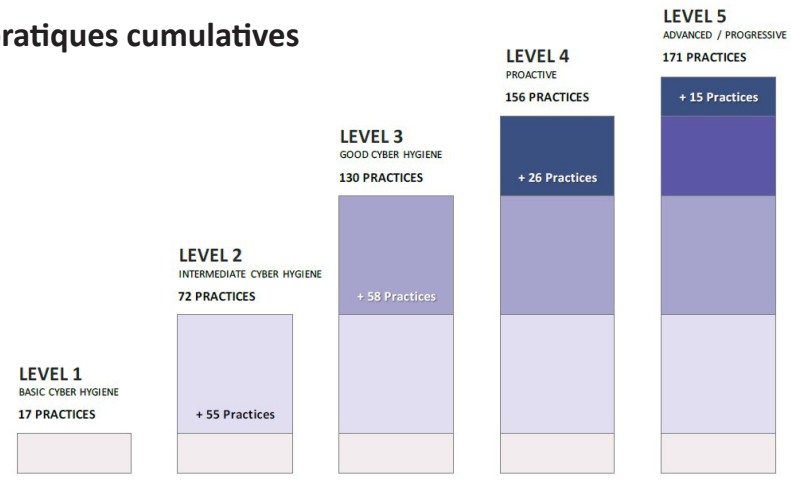


Figure 5. CMMC Practices Per Level

Le système chinois de crédit social

« Making it so that the trustworthy benefits at every turn and the untrustworthy can't move an inch »[1]. Par le système de crédit social (SCS), le gouvernement chinois entend évaluer la fiabilité des entreprises et de ses représentants afin de punir ceux qui se montreraient « indignes de confiance », et in fine d'influencer leurs comportements. Si l'attention des médias occidentaux s'est beaucoup portée sur le déploiement d'un système de notation des individus – parfois qualifié d'orwellien, l'objectif principal du SCS est l'autorégulation du marché en ciblant les entreprises qui souhaitent s'implanter en Chine. Ainsi, celles qui ne se conformeraient pas aux exigences gouvernementales pourraient être placées sur liste noire et se voir infliger une pluie de sanctions de la part des agences gouvernementales sur l'ensemble de leurs activités, voire sur leur personnel.

Qu'est-ce que le système de crédit social national ?

Lancé en 2014 par le Conseil des Affaires d'État, **le système de crédit social (SCS)** a pour objectif de **renforcer, le niveau général de confiance au sein de la société chinoise.** Il s'étend au-delà de la sphère financière : capacité de rembourser une dette, fiabilité d'une personne physique ou morale, sens des responsabilités civiques, structure de direction, licences administratives, antécédents en matière de conformité, etc.
Il est associé aux notions d'intégrité et de crédibilité.

Le SCS des entreprises **vise d'abord et avant tout à contrôler et influencer le comportement des entreprises sur le marché chinois.[2]**
L'originalité de ce système de régulation du marché tient dans sa rigidité (faible tolérance aux infractions), sa globalité (tous les aspects de la vie d'une entreprise) et son caractère interdépendant. Toutes les entreprises en Chine, nationales ou étrangères (actuellement plus de 2 000 françaises) ont toutes reçu, dès 2015, un numéro unique de crédit social (*unified social credit number*) devenant leur principal identifiant.

Comment fonctionne le SCS des entreprises ?

La base de données nationale, colonne vertébrale du système.

Chaque administration constitue un fichier, à partir de critères spécifiques définis aux échelons nationaux, locaux et sectoriels. Récoltées dans le fonctionnement habituel des administrations (ex. démarches administratives), ces données sont partagées *via* la ***Plateforme unique de partage des informations sur le crédit (*NCISP *Credit China,*** depuis 2015).
Ces données concaténées deviennent **stratégiques, dressant un portrait détaillé de l'entreprise et de ses capacités (détails technologiques, informations sur le personnel, actionnariats, cyber-sécurité, etc.)[3].**

Les systèmes de notation, indicateurs de fiabilité.

S'il n'existe pas encore de score national standardisé, l'évaluation d'une entreprise est directement et réciproquement liée à celle de ses partenaires, de ses représentants légaux et de son « personnel clé ».

.../...

[1] « Feuille de route sur la construction du système de crédit social », *Conseil des affaires d'État chinois,* 2014.
[2] Le SCS s'appuie sur les travaux de Lin Junyue qui présente, dès 1999, le crédit social comme une réponse à la méfiance qui règne sur le marché chinois après l'intégration brutale de la Chine dans l'économie mondiale (corruption généralisée, etc.).
[3] Entre 1 et 3% des données transférées par les entreprises et les autorités sont potentiellement de nature « sensible ». Antoine MOISSON, « Les implications du système de crédit social pour les entreprises », Direction générale du trésor, 4 octobre 2019.

Les listes noires/rouges, naming & shaming/praising.

Les agences gouvernementales ont la possibilité de placer sur liste noire les entreprises qui se trouvent sous leur juridiction, en cas de note négative, de non-respect des règles de conformité ou de condamnation officielle (pas de liste noire nationale, mais plutôt **des centaines de listes contrôlées par différentes agences gouvernementales).** L'objectif est **d'identifier les entreprises** (et les personnes) qui seraient **« indignes de confiance ». La durée de publication d'un mauvais score ou de la présence sur liste noire dépend de l'infraction commise.**

À l'inverse, **les listes rouges,** bien moins développées, **visent à louer les comportements exemplaires,** comme les bonnes relations professionnelles.
Les listes noires/rouges, ainsi que la plupart des informations liées au crédit social sont publiées sur les plateformes des organismes qui en sont à l'origine et **sur des plateformes nationales** et **privées** (ex. *Qichacha* ou *Tianyancha*).
Pour les entreprises, il s'agit du **Système national de publicité des informations de crédit social des entreprises** (NECIPS), mis en ligne en 2016.

Les mécanismes de sanctions/récompenses conjointes, bras armé du système de crédit social.

Chaque entreprise s'expose à des sanctions/récompenses de la part de l'entité qui l'a placée sur liste noire/rouge, et aussi de toutes les autres agences d'État qui ont signé un protocole d'accord avec ladite entité.
Les sanctions, qui **s'ajoutent aux pénalités juridiques et financières,** comprennent notamment **la réduction des quotas d'importation, l'interdiction de participer aux appels d'offre publics,** ou **l'interdiction d'ouvrir un site Internet.**

Les sanctions impactent aussi les représentants légaux et le « personnel clé » qui peuvent **subir, à titre personnel, les conséquences du mauvais score de leur entreprise** (ex. interdiction de prendre l'avion)[4] permettant ainsi de **maintenir une pression constante sur les entreprises** pour les inciter à se mettre en conformité au **risque de s'enfermer dans un cercle vicieux de sanctions en cascade.**

Quelles évolutions pour le SCS des entreprises ?

Étant donnée, la **portée quasi-illimitée de ce système, son développement et l'intégration de nouveaux critères en fonction des technologies disponibles mais aussi des objectifs politiques et économiques[5] ; le SCS devrait poursuivre son développement de façon incrémentale pour, notamment, intégrer de nouvelles capacités** comme l'IA ou le traitement de masse des données.

.../...

Exemple : « Aladin » de HiggsCredit attribue une note allant de 0 à 1000 à partir des informations générales, du « degré de confiance de l'entreprise déterminé par son 'comportement' social », du niveau d'activité, des informations financières, des relations commerciales et des partenariats. La plateforme fournit, par ailleurs, des informations sur l'actionnariat, la santé financière et les profils des employés, ainsi que des articles de presse. Tous ces géants du numérique (HiggsCredit, Alibaba, Baidu Credit, etc.) ont signé des accords d'échange de données avec le gouvernement, dont les modalités restent inconnues.

Vers plus d'intégration

Le gouvernement prévoit le déploiement **d'une nouvelle base centrale : le « National 'Internet + Monitoring' System »[6], afin d'intégrer toutes les informations relatives au crédit social issues des agences gouvernementales et des plateformes de notation privées ainsi que les données de l'appareil de surveillance.**

Le risque de dérives

Certains **critères pourraient être utilisés pour cibler,** à des fins politiques, **les entreprises étrangères.** À cet égard, **la liste noire à venir des entités « très peu fiables »** (*heavily distrusted entites*), développée au niveau national par la *State Administration for market regulation*, peut apparaitre comme un levier politique.

D'autres réglementations pourraient servir de base pour cibler les entreprises étrangères comme le projet de régulation présenté en 2019 par la *Cyberspace Administration of China* qui vise **les entités ayant relayé des informations jugées sensibles, notamment celles ayant une « mauvaise influence sur la société », et les entreprises qui diffuseraient des « rumeurs »[7].**

Les ambitions d'exportation à l'international du SCS

Mettant à profit son projet des **« Nouvelles routes de la soie »,** la Chine souhaiterait **exporter son système pour contrebalancer l'influence des grandes agences de notations occidentales** et *in fine* **changer le système international de notation pour un système basé sur sa définition de la fiabilité.**
Plusieurs pays en Asie et au Moyen-Orient **se sont ainsi engagés dans des projets de collaboration** (ex. l'Arabie saoudite).

Exemple : En 2018, la Chinese Civil Aviation Administration a accusé plusieurs compagnies aériennes de « malhonnêteté sérieuse » pour avoir listé Taïwan, Hong-Kong et Macao sur leurs sites web sans mentionner leur filiation à la République populaire de Chine.

[4] Ces sanctions peuvent se poursuivre après la fin du contrat avec l'entreprise. Voir « An introduction to China's Corporate Social Credit System », *op.cit.*
[5] La liste des « délits » passibles d'une inscription sur liste noire pourrait aussi s'allonger pour inclure des comportements pourtant légaux et des critères pour influencer les croyances religieuses, les opinions politiques et les choix des consommateurs. SCHAEFER, YIN, et al., *op.cit.*
[6] Encore aujourd'hui en phase de tests, cette nouvelle base aurait dû être opérationnelle à la fin de l'année 2019. Voir MOISSON, *op.cit.*
[7] SCHAEFER, YIN, et al., *op.cit.*

Vague de cyberattaques cyber-djihadistes

Depuis septembre 2020, plusieurs sites web d'entités françaises, y compris d'entreprises, ont été touchés par une série de défigurations[1] d'inspiration islamiste. Cette campagne d'attaques a visé principalement des serveurs web présentant des vulnérabilités dans leurs configurations ou dans la mise à jour de certains de leurs composants. Ces attaques, aisément automatisables et opportunistes ne demandent pas un haut niveau technique pour être perpétrées. Néanmoins, elles peuvent donner lieu à des exfiltrations de données en cas de mauvais cloisonnement dans l'architecture du réseau.

Outre ces attaques par défiguration, plusieurs campagnes de *trolling*[2] sur les réseaux sociaux ont été observées. Bien que ne présentant pas de menaces immédiates pour les systèmes d'information, elles peuvent porter atteinte à l'image de marque de l'entreprise. Plusieurs milliers de messages appelant au djihad et aux tueries de masse en France ont ainsi été diffusés.

Enfin, quelques cas d'attaques par « déni de service distribué » (DDoS) ont été relevés en France. Ces attaques, qui visent à rendre indisponible un service ouvert sur internet en multipliant les requêtes de connexion, sont assez communes dans le cyberespace, et ne sont pas propres aux groupes cyber-djihadistes.

La DRSD vous alerte sur ces récentes campagnes d'attaque qui, bien que diminuant en intensité, peuvent faire courir un risque pour l'intégrité et la disponibilité des systèmes d'information. De plus, une attaque réussie peut porter atteinte à l'image d'une société.

Recommandations :

- cloisonner les systèmes d'information ayant un accès Internet du reste du réseau de l'entreprise ;
- maintenir à jour les infrastructures informatiques et ce le plus fréquemment possible, notamment celles exposées sur internet ;
- mettre en place des mots de passe robustes pour les comptes sur les réseaux sociaux et idéalement instaurer une authentification à deux facteurs ;
- mettre en place une veille des comptes ouverts sur les réseaux sociaux ou sites internet et avoir une procédure de gestion rapide d'incidents en cas de campagnes de *trolling* ou de défiguration.

En cas d'attaque, contactez sans attendre la DRSD.

[1] Une défiguration est une attaque cybernétique qui vise à pénétrer le serveur d'un site web pour modifier le contenu des pages affichées.
[2] Campagnes qui consistent à saturer un compte sur un média social de publications subversives ou véhiculant des idées contraires aux idéaux portés par le compte.

Gardons contact

Restons en contact

Direction

Contre Ingérence Économique

drsd-cie-sensibilisation.contact.fct@intradef.gouv.fr