Lettre d'information économique

Sommaire

Octobre 2020

Editorial

Contre-ingérence et sécurité économiques : des outils de gestion de crise

En économie, comme en bien d'autres domaines, l'*immobilisme* et l'*indécision* contreviennent au succès et à l'atteinte des objectifs de qualité et de compétitivité. Or, la crise sanitaire et ses effets ont engendré une forme de **sidération**, qui a cristallisé l'activité pendant plusieurs semaines et considérablement **réduit la visibilité** sur les marchés. Il est soudainement devenu encore plus difficile qu'auparavant de décider avec clairvoyance pour « rendre l'avenir possible » , à défaut de le prévoir.

A n'en pas douter, l'activité économique, au cours des mois qui viennent, nous verra, acteurs publics et acteurs privés, exposés à un **état de crise permanent**, impliquant une gestion avisée, pragmatique et réactive.

Dans ce contexte, les acteurs étrangers les plus puissants vont tenter de gagner encore davantage d'ascendant, la sécurité économique constituera **un mode de vigilance et d'action incontournable.** La lutte contre les ingérences étrangères, l'anticipation des tentatives de prédation financière, le suivi du détournement du droit au profit du contrôle des exportations, le juste discernement des partenariats souhaitables, la détection des atteintes cybernétiques, la préservation des savoir-faire, de la recherche et plus généralement des données numériques, constitueront, plus que jamais, des défis majeurs.

La DRSD est consciente des tendances qui se dessinent. Dans un esprit de coopération évident avec les autres acteurs de l'Etat qui concourent à « faire gagner l'équipe France », la DRSD s'est donnée comme objectif d'y voir aussi clair que possible, en étant **toujours plus en contact avec les entreprises.**

En situation de crise, il faut serrer les rangs et partager l'information. Au bon sens doit s'ajouter une forme de combativité accrue. Cette lettre, élaborée à votre profit direct, a pour objectif d'y contribuer.

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

La contre-prolifération

Comme le rappelle le code de la défense, la DRSD est le « service de renseignement dont dispose le ministre des armées pour assumer ses responsabilités en matière de sécurité du personnel, des informations, du matériel et des installations sensibles » en lien direct ou présentant un intérêt pour la défense nationale.

A ce titre, la DRSD participe également, à l'instar d'autres services, à l'effort national de lutte contre la prolifération des armes de destruction massive et de leurs vecteurs.

Prolifération (définition) : propagation illégale et non contrôlée d'armes de destruction massive qu'elles soient nucléaires, radiologiques, biologiques, chimiques ou l'un de leurs vecteurs (missiles de croisière ou balistique, engins explosifs, aéronefs, drones, etc.), via des réseaux d'acquisition clandestins et/ou déguisés de composants, matériaux, machines, savoir-faire, connaissances, etc. concourant au développement, à la fabrication, la mise en œuvre, le stockage ou la dissimulation de ces armes.

Mission du Service

Fidèle à sa devise - « renseigner pour protéger », la DRSD s'emploie à actualiser et accroître ses connaissances concernant les programmes et acteurs proliférants afin de surveiller, d'identifier, de prévenir voire d'entraver toutes les tentatives d'acquisition de biens matériels ou immatériels auprès d'une entreprise, d'un établissement d'enseignement supérieur et de recherche, d'un laboratoire ou de toute autre organisation intéressant la défense.

Un échange de bons procédés

Afin que son action puisse être la plus efficace possible, la DRSD s'attache à établir et conserver un dialogue permanent avec les entités dont elle assure le suivi. En effet, en matière de contre-prolifération, la captation et le détournement de savoir-faire sensibles se révèlent aussi préjudiciables que l'acquisition de matériels elle-même. Ils sont, de surcroît, beaucoup plus complexes à entraver car, intangibles par essence, ils peuvent échapper aux mécanismes de contrôle à l'export tels que ceux mis en œuvre pour limiter la prolifération des biens jugés sensibles et duaux.

Afin de rappeler l'importance cruciale de la remontée d'alerte par la chaîne de sécurité compétente, la DRSD propose régulièrement des actions de sensibilisation au profit des officiers de sécurité, cadres, enseignants-chercheurs, techniciens dont les profils et compétences sont susceptibles d'intéresser un pays proliférant.

La DRSD s'attache, par ailleurs, à prendre en compte effectivement tout fait qui lui est signalé : courriels suspects où sont posées des questions sur un produit, prise de photos aux abords d'un site industriel sensible, candidature d'un doctorant de nationalité étrangère, etc.

Forte de sa connaissance des briques technologiques recherchées par les pays proliférants, la DRSD est en mesure, grâce aux signalements des officiers de sécurité, d'effectuer des levées de doute sur les profils pour écarter ceux pouvant présenter des risques et d'assurer un suivi durable des ressortissants étrangers présents dans les établissements intéressant la défense afin d'identifier tout incident de sécurité et/ou comportement anormal.

La DRSD accompagne également les entreprises, écoles et laboratoires dans leurs interactions avec l'étranger : visite d'une délégation étrangère sur site, participation à un séminaire ou un salon à l'étranger, accueil d'étudiants ou doctorants étrangers, etc. Dans ce cadre, elle est en mesure d'apporter une expertise et de proposer des conseils adaptés.

Inspections et conseils

L'accompagnement des industries de défense en période de crise

Dans le cadre du volet « protection » de sa mission de contre-ingérence économique, la DRSD est amenée à inspecter les industriels de défense détenteurs de secrets de la défense nationale et ceux s'inscrivant dans le cadre du dispositif de protection du potentiel scientifique et technique de la Nation (PSTN). Malgré les perturbations significatives sur la programmation de ces inspections, liées à la crise pandémique Covid 19, le centre de conseil, de la prévention et des inspections (CCPI) ainsi que le centre technique et cyber (CTC) se sont attachés à maintenir le lien avec les industriels en leur prodiguant notamment des conseils adaptés dans ce contexte de crise.

Pour des raisons évidentes, l'appréhension et la gestion de cette crise ont varié selon la taille des entreprises concernées. Les grands groupes ont activé leur cellule de gestion de crise et déroulé leur plan de continuité d'activité pour maintenir leurs activités essentielles, et mobilisé l'ensemble de leurs structures de sécurité. Les PME et TPE, quant à elles, ont plus difficilement absorbé les impacts de cette pandémie, à laquelle elles ont dû faire face à l'aide des seuls outils dont elles disposaient et en sollicitant des responsables cumulant souvent plusieurs fonctions, outre la sécurité.

Conscients de ces situations très hétérogènes et soucieux de pouvoir, en dépit des circonstances, continuer à rencontrer et conseiller leurs partenaires industriels dans la réalisation de leurs engagements contractuels avec le ministère des armées, les équipes d'inspection-conseil de la DRSD se sont adaptées pour leur apporter leur soutien.

En effet, en liaison avec chacune des directions zonales et des postes de la DRSD, qui constituent les interlocuteurs de proximité des entreprises, le CCPI et le CTC ont déployé un nouveau type de mission : la visite-conseil, conduite sur une demi-journée.

Initiée en région parisienne, cette formule sera étendue à l'ensemble de la métropole jusqu'à fin décembre 2020. Il s'agit pour nos experts de conseiller les entreprises en réalisant une évaluation précise de la situation de protection et de sécurité de chaque entité. Différents aspects sont abordés, telles que les difficultés spécifiques engendrées par la crise sanitaire, la continuité d'activité, l'exécution des contrats de défense, les aspects liés aux chaînes de sous-traitance, les incidents ayant pu être constatés, mais également le dispositif de protection physique des locaux, sans omettre la sécurité des systèmes d'information, dont la prégnance s'est trouvée accrue par les vulnérabilités supplémentaires induites par le recours massif au télétravail.

En la matière, la DRSD conseille les entreprises sur la sécurisation de leur SI en s'appuyant notamment sur l'utilisation de logiciels agrées par l'ANSSI, comme *Cryhod* pour le chiffrement des postes nomades ou *Tixeo* pour les visioconférences plutôt que des solutions grand public plus connues. Elle leur recommande également de sensibiliser davantage leurs collaborateurs aux risques cyber.

Ces visites-conseils permettent d'identifier des vulnérabilités critiques, d'échanger avec la direction du site, d'accompagner, de la manière la plus adaptée et concrète possible, chacun des partenaires industriels dans la gestion de crise, la continuité d'activité et les réponses aux problématiques émergentes.

Les réseaux sociaux

des vecteurs d'ingérence privilégiés

Les réseaux sociaux professionnels, tels que *Linkedin* ou *Viadeo*, sont considérés comme des outils de rayonnement par les entreprises et leurs collaborateurs afin de communiquer, recruter ou encore créer des liens professionnels. Ils leur permettent, en effet, d'accroître leur visibilité en partageant des informations. Toutefois, ces échanges demeurent souvent peu maîtrisés et peuvent être exploités par des acteurs malveillants de tous types (services de renseignement, concurrents déloyaux, criminels, mouvements subversifs).

Les réseaux sociaux constituent des vecteurs de choix pour les acteurs malveillants cherchant à identifier des cibles à haute valeur pour mener des opérations d'ingénierie sociale. Or, force est de constater que les collaborateurs des entreprises ont tendance à diffuser de plus en plus d'informations, y compris sensibles, concernant leurs fonctions et leurs travaux.

Le type d'approche souvent constaté prend généralement la forme d'une prise de contact virtuelle sur un réseau social avant de réorienter l'échange sur des plateformes de messagerie instantanée permettant des interactions plus fluides. Le prétexte varie selon le profil de la cible : proposition de rendez-vous, invitation à un séminaire à l'étranger ou encore proposition d'emploi. La finalité de la prise de contact est d'obtenir de la part de la personne ciblée, souvent à son insu, des informations sensibles sur l'entreprise, soit immédiatement, soit dans le cadre d'une relation à plus long terme. L'auteur de l'approche peut également exploiter cette relation pour intégrer des cercles professionnels afin d'approcher d'autres cibles qu'il ne peut atteindre directement.

Pour les acteurs malveillants, la diffusion non maîtrisée d'informations, facilite donc la collecte d'informations sur l'environnement d'une entreprise, et *a fortiori* d'une personne, afin de concevoir et mener des ingérences aussi sophistiquées qu'initialement discrètes. À titre d'exemple, des cyber-attaquants profitant d'une campagne de recrutement peuvent adresser aux services des ressources humaines des *curriculum vitae* dissimulant des maliciels.

La DRSD observe une amélioration constante des techniques d'ingénierie sociale et d'approches humaines : arnaques « au président[1] », « aux faux fournisseurs », etc. Il est démontré que cet essor est rendu possible grâce à l'exploitation des informations parfois sensibles diffusées sur les réseaux.

Quelques recommandations...

Afin de maîtriser les risques d'ingérences liés à l'utilisation des réseaux sociaux, la DRSD préconise notamment:

- d'informer les collaborateurs des modes opératoires offensifs mettant à profit les réseaux sociaux professionnels ;
- de sensibiliser les collaborateurs sur les risques liés à la diffusion non maîtrisée d'informations, tant professionnelles que personnelles, sur ces plateformes ;
- en cas de sollicitation d'un collaborateur, de vérifier la légitimité de l'émetteur ;
- en cas de sollicitation malveillante ou de doute, de rendre compte à l'officier de sécurité et à la DRSD ;
- de sensibiliser les collaborateurs à la gestion des pièces-jointes d'émetteurs inconnus ;
- de cloisonner les systèmes d'information ayant un accès Internet du reste du réseau de l'entreprise.

[1] Ces attaques consistent à usurper l'identité d'un cadre de la société ou d'un fournisseur afin des fonds sous prétexte d'un impératif aussi urgent que confidentiel.

Lancement du Diagnostic Cyber-Défense

Le plan ACTION PME du ministère des Armées vise à aider les PME et ETI à travailler avec le ministère des Armées pour maintenir la supériorité opérationnelle des armées françaises et répondre à leurs besoins nouveaux.

Florence Parly, ministre des Armées, a annoncé lors de son déplacement à Rennes le 8 septembre 2020, la création du Diagnostic Cyber-Défense (« Diag Cyber »). Il s'agit d'une mesure du plan Action PME qui s'inscrit dans le prolongement de la convention signée entre le ministère des Armées et ses maîtres d'œuvre industriels pour sécuriser le développement, la production et la maintenance des systèmes d'arme.

Ce dispositif d'aide à la cyber sécurisation des PME et des ETI de l'industrie de Défense permet à ces entreprises de renforcer la chaîne cyberdéfensive de « bout en bout » pour réduire les vulnérabilités de l'écosystème de défense aux cyber-attaques.
Il permet ainsi aux PME et ETI d'identifier les risques numériques liés à leur entreprise, d'évaluer le niveau de sécurité de leurs systèmes d'information, d'identifier les failles éventuelles et d'accompagner la mise en œuvre, le cas échéant, d'un plan de remédiation, qui est audité *a posteriori*.
Le « Diag Cyber » consiste en une prestation d'audit et de conseil et éventuellement d'accompagnement à la mise en œuvre des recommandations. Les prestations seront réalisées par des sociétés labellisées par l'ANSSI ou par des sociétés qui appliquent des méthodes d'audit similaires validées par la DGA.

Ce dispositif, appuyé par la DRSD, est géré par la Direction générale de l'armement (DGA) et opéré par Bpifrance. Il est financé par le ministère des Armées à hauteur de 4,5 millions d'euros.

La DGA vérifie et valide, selon les critères d'éligibilité, toutes les demandes des PME et ETI intéressées par ce dispositif. Cette pré-qualification permettra de bénéficier d'une prise en charge par le ministère des Armées du coût de la prestation à hauteur de 50% et pouvant s'élever jusqu'à 14 000 euros HT.

Pour en savoir plus sur les conditions de ce dispositif, les entreprises sont invitées :

- à consulter la plaquette de présentation (https://www.defense.gouv.fr/content/download/592510/10035496/diagnostic_cyber_dga_2020.pdf) ;
- à se rendre sur la plateforme en ligne pour initier les demandes d'octroi du dispositif (www.demarches-simplifiées.fr/commencer/diagnostic-cyber-defense).

Gardons contact

Restons en contact

Direction zonale Île de France

prsd-villacoublay.cmi.fct@intradef.gouv.fr