Lettre d'information économique

Sommaire

Juin 2021

Editorial

L'année 2020 aura été fortement marquée par une crise sanitaire sans précédent qui a déstabilisé les entreprises et leur environnement. Cette situation exceptionnelle a été de nature à modifier les modes d'ingérence, désormais plus sophistiqués et polymorphes, comme le démontrent les cas concrets présentés dans le panorama des ingérences pour l'année 2020.

Dans ce contexte de crise et compte tenu des contraintes qui en découlent, la DRSD, soucieuse d'offrir des services adaptés à vos besoins, met à votre disposition un MOOC spécifiquement dédié à aider vos équipes à s'approprier la nouvelle IGI 1300 à partir du 1er juillet 2021.

La DRSD s'est également engagée dans un protocole de coopération avec le Groupement d'Intérêt Public Action contre la cybermalveillance (GIP ACYMA) pour offrir son soutien et son expertise en cybersécurité.

Enfin, la DRSD rappelle que les CERT (*Computer Emergency Reponse Teams*) sont des prestataires précieux en matière de cybersécurité et de cyberdéfense.

J'ai demandé à toutes mes équipes, présentes à vos côtés, de rester mobilisées pour vous accompagner dans vos démarches de prévention et de protection.

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

Panorama

des ingérences 2020 et cas concrets

L'internationalisation des échanges a polarisé les rapports de force et exacerbé la course à la compétitivité. Dans ce contexte, l'acquisition d'informations concurrentielles, technologiques ou d'innovations relève désormais d'une stratégie essentielle voire incontournable. À l'échelle mondiale, l'impact de la crise sanitaire a notamment incité l'ensemble des acteurs étatiques ou économiques à mettre en place des moyens de protection de leurs actifs et des plans d'acquisition de savoirs ou de savoir-faire.

Le nombre d'ingérences directes ou indirectes a augmenté, tant vers les industriels que les établissements de recherche de la BITD (base industrielle et technologique de défense) notamment sous la forme d'actions de cyberattaques multiples ou de techniques d'influence et de débauchage, sans oublier les manœuvres capitalistiques ou d'ingénierie juridique et réglementaire.

Sur fond de rivalité commerciale mondiale, les secteurs les plus touchés demeurent les filières industrielles de haute technologie de défense et de sécurité, les technologies de l'information et de la communication, notamment dans les domaines de l'aéronautique et du spatial.

Les grandes puissances continuent de développer des stratégies très offensives en vue d'acquérir des informations à haute valeur ajoutée, tandis que d'autres nations, moins couramment citées, mettent en place des stratégies structurées et planifiées d'acquisition d'informations stratégiques, afin de pallier leurs retards technologiques et s'intégrer à la compétition mondiale.

Durant cette crise sanitaire, le recours rapide et massif au télétravail a représenté une réelle opportunité pour les cybercriminels contribuant ainsi à une augmentation du nombre de cyberattaques de toutes sortes (chantage à la divulgation de données, rançongiciels, installations de malwares, fraudes aux fournisseurs ou au président).

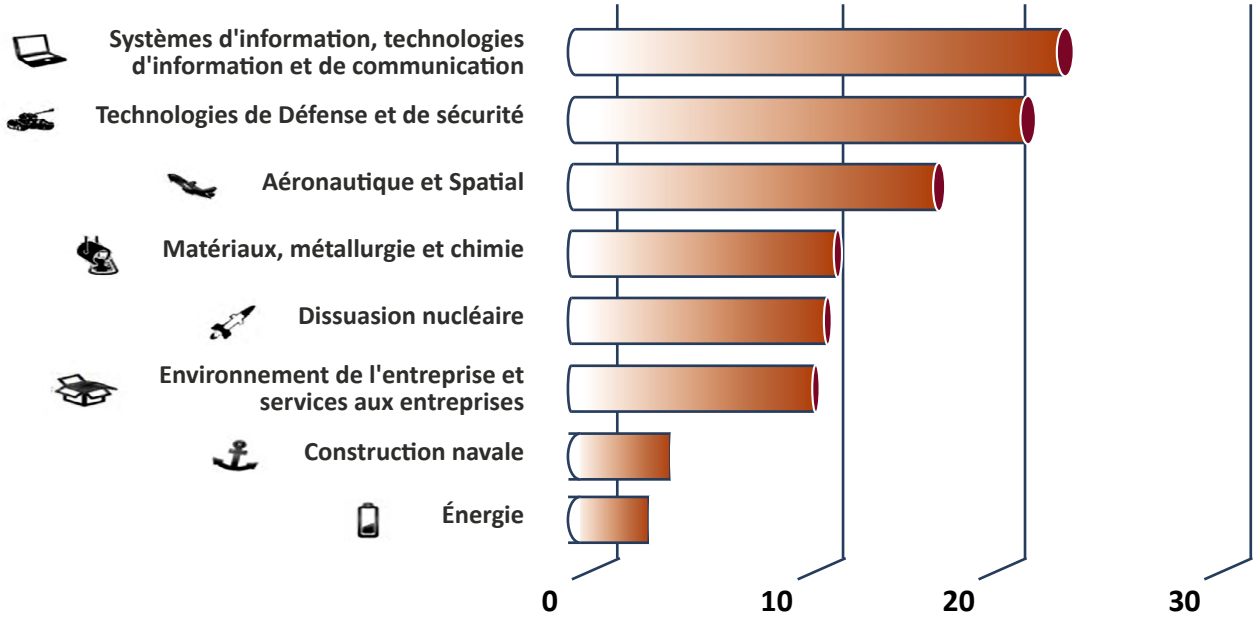
De nombreux acteurs malveillants ont également profité de cette situation particulière pour identifier et exploiter systématiquement les vulnérabilités ou fragilités engendrées par la crise, notamment chez les sous-traitants de défense. Certains acteurs étatiques ou économiques étrangers n'ont pas hésité, en effet, à maintenir une posture offensive à l'encontre de sociétés de défense françaises et de leurs chaînes d'approvisionnement en utilisant notamment la promesse d'investissements de capitaux ou encore des moyens juridiques et réglementaires à portée extraterritoriale générant des procédures d'audits très intrusifs.

Panorama

des ingérences 2020 et cas concrets

Sophistication des cyber attaques

Domaines ciblés



Illustrations par des cas concrets

Exfiltration et chiffrement des données

En raison de la crise sanitaire, une ETI spécialisée dans la mécanique de précision a eu recours à l'utilisation du télétravail. Elle a été victime d'une attaque informatique ciblée, en deux temps, par un attaquant de haut niveau, en raison d'un déploiement de travail à distance rapide et peu sécurisé. La première attaque a permis l'exfiltration de plusieurs dizaines de giga-octets dont des données à caractère personnel. La seconde attaque est survenue à quelques jours d'intervalle pour chiffrer l'ensemble des données de l'entreprise paralysant ainsi toutes ses activités. L'ensemble du réseau informatique est resté hors d'usage pendant près d'une semaine. Cela a entraîné de graves répercussions pour sa réputation et sur son activité, dont des pertes de marchés.

« Arnaque au président »

Depuis l'année 2020, la DRSD a noté une multiplication des « anarques au président » sophistiquées contre la BITD. Plusieurs sociétés ont, en effet, été les cibles d'actions particulièrement élaborées, notamment dans leur phase de préparation. Ces tentatives d'escroquerie ciblant des dirigeants des entreprises ont démontré une parfaite maîtrise des techniques d'ingénierie sociale et de collecte d'informations par les attaquants. Leur amélioration qualitative augmente leur probabilité de réussite et constitue par conséquent une menace croissante pour toutes les entités sous-traitantes de la BITD, en particulier celles déjà financièrement fragilisées par la crise pandémique.

Vulnérabilité des petites entités sans structure juridique

Une société, sous-traitante de défense employant une centaine de personnes et spécialisée dans l'électronique, a développé son marché à l'international. Après avoir vendu l'un de ses produits à une société étrangère, la PME a identifié dans le catalogue de produits d'un concurrent un produit en tout point identique au sien.

La société innovante ne possède pas de dispositif de protection juridique lui permettant de lutter contre le *retro engineering* et le produit en question n'a pas fait l'objet de dépôt de brevet ni en France ni à l'international. Situation qui, de surcroît, a permis au concurrent de déposer plainte à son encontre pour plagiat.

Investissement étranger dans le capital

Un sous-traitant de plusieurs entreprises françaises, spécialisé dans la mécanique et le blindage a été fragilisé par la crise sanitaire et n'a pu obtenir de prêt garanti par l'Etat.

En 2020, il a fait l'objet d'un audit organisationnel diligenté par son actionnaire étranger majoritaire. Les résultats de cet audit fixent au sous-traitant des objectifs jugés irréalistes par son dirigeant. L'audit intervient alors que cet actionnaire majoritaire envisage de céder 15% de ses parts à un autre groupe, issu du même pays d'origine, et qui pourrait ainsi, d'ici trois ans, prendre le contrôle à hauteur de 49 à 50% du capital social du sous-traitant. Les conséquences directes pour le sous-traitant sont la perte d'actifs ainsi que de savoir-faire transférable sur le site de production étranger du second actionnaire. Cette situation préoccupante contraindrait les donneurs d'ordres à recourir à des prestataires et sous-traitant étrangers engendrant une perte de souveraineté.

Audits comptables et financiers

Dans le cadre de leurs missions, certains cabinets sont mandatés contractuellement pour mener des audits comptables et financiers au sein des entreprises françaises à la suite de la publication annuelle ou semi annuelle de leurs comptes. Certains cabinets, étrangers, n'hésitent pas, au cours de ces audits, à se montrer particulièrement intrusifs en tentant de capter de l'information non relative au domaine comptable ou financier, mais relevant plutôt d'autres domaines d'intérêt (organisation, prospectives de futurs marchés, recherche et développement, etc.). De nombreuses sociétés de la BITD ont fait l'objet de ce type de manœuvre. Malgré les fortes réticences des chaînes sécurité-sûreté, certains cabinets d'audits ont réussi à obtenir des éléments techniques ou organisationnels précis. La divulgation non appropriée d'information fragilise les structures et leur exploitation met en péril la pérennité de l'organisation.

Un CERT pour tous

Les systèmes d'informations sont devenus la cible de groupes attaquants souhaitant voler les données sensibles des acteurs industriels. En moyenne, une entreprise victime d'une cyberattaque a besoin de deux ans pour restaurer son système d'information. Face à la hausse des cyberattaques de tous types, la prise en compte des enjeux de cybersécurité est devenu indispensable. Dans le cadre du Plan de Relance, le Président de la République a annoncé, le 18 février 2021, un plan global dédié à la cybersécurité prévoyant notamment 720 millions de financement public d'ici 2025.

L'un des éléments de cette prise en compte repose sur la capacité humaine et technique à détecter et circonscrire les cyberattaques dans une logique de défense périmétrique. À ce titre, le recours aux CERTs (*Computer Emergency Response Teams*) aussi appelés CSIRT (*Computer Security Incident Response Team*) apparait comme l'outil adapté et incontournable.

Disposant d'une place centrale dans l'écosystème cyber, les CERTs centralisent les demandes d'assistance, assurent la réaction aux incidents de sécurité, suivent les vulnérabilités, réalisent une veille technologique, et coopèrent avec leurs partenaires.
Ces structures permettent ainsi l'alimentation des SOC (*Security Operations Center*), et la bonne conduite de la cyber sécurité des entités de leurs périmètres. Un CERT est ainsi le point de contact privilégié, interne comme externe, pour les questions de cyber sécurité.

La place d'un CERT dans l'organisation peut être interne ou externe, selon la politique et les moyens de chaque entreprise. Cependant, pour les entreprises ne disposant pas des moyens pour s'assurer les services d'un CERT, d'autres possibilités existent. Ainsi, l'agence nationale de sécurité des systèmes d'information (ANSSI) contribue à la constitution de structures régionales ou sectorielles. Parmi celle-ci, le Centre de Ressource Régional Cyber (C2RC) accessible aux entreprises et collectivités du sud de la région PACA, ou le CERT Maritime qui couvrira le périmètre des navires, ports et armateurs en France.

La DRSD encourage tout acteur de la sphère « défense » à prendre en compte cette organisation dans sa défense cyber et identifier ainsi le CERT qui correspond le mieux à ses moyens, son activité et la menace qui pèse sur celle-ci. Le but est d'intégrer le CERT le plus tôt dans la politique de cybersécurité.

**Observation de la menace, prévention du risque et assistance aux victimes :
La ministre des Armées aux côtés de cybermalveillance.gouv.fr**

Le 4 mars dernier, la ministre des Armées a signé un protocole de coopération avec le Groupement d'Intérêt Public Action contre la cybermalveillance (GIP ACYMA) qui concrétise son engagement au sein du dispositif national d'observation, de prévention et d'assistance aux victimes cybermalveillance.gouv.fr.

Créé en 2017 par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et le ministère de l'Intérieur, le GIP ACYMA est issu de la stratégie nationale pour la sécurité numérique de 2015 pour apporter une aide structurée à toutes les composantes de la société (particuliers, entreprises, collectivités territoriales, etc.) et faire face à l'explosion de la cybercriminalité et de la cyber-délinquance.

Le GIP ACYMA rassemble une cinquantaine de membres (acteurs étatiques, représentations professionnelles, associations de consommateurs et d'aide aux victimes, opérateurs, éditeurs, assureurs…) qui concourent tous aux missions d'observation de la menace cyber, de la prévention des risques numériques et de l'assistance aux victimes.

En rejoignant ce dispositif, le ministère des Armées fait bénéficier cybermalveillance.gouv.fr de ses moyens de soutien logistique et de communication ainsi que de ses ressources et compétences spécifiques pour lutter contre les menaces cybernétiques.

Partenariat

cybermalveillance.gouv.fr

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

La DRSD, service de renseignement spécialisé dans la contre-ingérence, renforce la cyberdéfense de la PME aux grands groupes

Dans le cadre de cet accord, le ministère des Armées a désigné la DRSD pour le représenter et coordonner les actions de coopération avec ses différentes composantes. A ce titre, la DRSD a détaché un officier de contre-ingérence à plein temps au sein du GYP ACYMA afin de renforcer les synergies dans l'ensemble des régions et soutenir tout type d'entité en lien avec la défense.

Fort de son maillage territorial, la DRSD assure une coopération de proximité avec l'ensemble des acteurs de la base industrielle et technologique de la défense et ceux de la cybersécurité afin de contribuer au renforcement des capacités de résilience des entreprises pour préserver les intérêts stratégiques de défense. La DRSD fournit donc son appui et son expertise à travers des missions d'audits et de conseils mais aussi en développant des produits et services de sensibilisation aux risques numériques destinés aux comités exécutifs et collaborateurs des entreprises de toutes tailles ainsi qu'à tout organisme en lien avec la défense.

1- DIAGNOSTIC EN LIGNE

Victime d'acte de cybermalveillance ? Nous vous aidons à qualifier votre problème.

2 - DES CONSEILS ET SOLUTIONS

ET / OU

Des conseils et solutions vous sont propsés pour résoudre votre problème.

Vous pouvez faire une demande de mise en relation avec un professionnel spécialisé.

« S'il existe bien un espace où la malveillance ne dort jamais, un espace où chacun d'entre nous peut devenir la cible, […] c'est bien le cyber espace » Florence Parly, ministre des Armées.

SE PROTÉGER

Consultez nos bonnes pratiques et conseils pour vous protéger des cybermenaces

SIGNALER

Vous souhaitez signaler une escroquerie en ligne ou un contenu illicite sur Internet ?

DÉPOSER PLAINTE

Vous souhaitez déposer plainte suite à une cybermalveillance ?

Partenariat

cybermalveillance.gouv.fr

La plateforme cybermalveillance.gouv.fr offre de nombreux supports de sensibilisation et guides de bonnes pratiques accessibles gratuitement, ainsi que la possibilité de réaliser, en ligne, un diagnostic des vulnérabilités du système d'information assorti de conseils de première urgence. Pour mieux toucher les entreprises, cybermalveillance.gouv.fr a également développé le label Expert Cyber en partenariat avec l'AFNOR pour mettre à disposition des prestataires de confiance référencés sur la plateforme et qui démontrent une expertise avérée en matière de cybersécurité. A ce jour, 55 prestataires labellisés sont répertoriés pouvant accompagner, au besoin, les entreprises ou autres entités dans la mise en œuvre de projets de sécurisation de leurs infrastructures informatiques.

Quelles sont les missions d'un professionnel référencé ?

1. Assister les victimes de cyber-attaques

En agissant directement et concrètement sur le terrain auprès des victimes qu'ils assistent, les professionnels en sécurité informatique référencés constituent le premier rempart de la chaîne de la cybersécurité.

2. Sensibiliser les différents publics à la sécurité informatique

En tant que prestataires référencés par cybermalveillance.gouv.fr, les professionnels en sécurité informatique se positionnent de facto comme des vecteurs de sensibilisation de proximité au risque numérique, en partageant par exemple les contenus d'information et de prévention produits par le dispositif.

3. Contribuer à la lutte contre les cybermalveillances

En remontant leurs observations du terrain vers le dispositif cybermalveillance.gouv.fr au travers de leurs rapports d'intervention pour lui permettre d'adapter ses messages de prévention et d'initier les actions nécessaires.

IGI 1300

Une formation animée à votre disposition

La réglementation relative à la protection du secret de la défense nationale, fait l'objet d'une profonde transformation.

Un nouveau système de classification à deux niveaux

Le décret du 2 décembre 2019 indique qu'à compter du 1er juillet 2021, il n'existera plus que deux niveaux de classification, utilisés en fonction du degré de sensibilité des données considérées : le niveau Secret et le niveau Très Secret.

Chacun de ces niveaux accorde une protection proportionnée au risque encouru en cas de divulgation des informations et supports (ISC) qu'ils couvrent :

- le niveau **Secret** protège les informations et supports dont la divulgation, ou auxquels l'accès, est de nature à porter atteinte à la défense et à la sécurité nationale ;
- le niveau **Très Secret** concerne ceux dont la divulgation aurait des conséquences exceptionnellement graves pour la défense et la sécurité nationale.

Globalement, la nouvelle IGI 1300 vise à rendre plus rigoureuses les règles de classification afin d'éviter la classification tout en renforçant la protection des documents classifiés.

Un MOOC animé spécifique dédié aux nouvelles dispositions

Afin de faciliter l'acquisition de ces nouvelles dispositions, la DRSD met à la disposition de tous un outil de formation animé et spécialement développé à cet effet.

Ce cours en ligne (Mooc) a été conçu notamment pour aider toutes les entités de la Base industrielle et Technologique de la Défense (BITD) et particulièrement celles qui n'ont pas l'habitude de traiter des informations classifiées. En permettant au plus grand nombre de personnes habilitées dans la sphère défense de se former aux règles relatives à la protection du secret, la DRSD souhaite renforcer l'ensemble de la chaîne afin de garantir une meilleure sécurité des informations classifiées.

Le cours en ligne de la DRSD a été élaboré pour expliquer les nouvelles dispositions contenues dans l'IGI 1300 et pour transmettre les bonnes pratiques auprès des personnes habilitées.

Pour le découvrir, rendez-vous sur www.drsd.defense.gouv.fr, **à compter du 1er juillet 2021.**

Gardons contact

Restons en contact

Contre Ingérence Économique

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