Lettre d'information économique

Spéciale
ÉCONOMIE DE GUERRE

Sommaire

Editorial

De la « guerre économique » à l' « économie de guerre »

Mesdames, Messieurs,

La résurgence récente de tensions internationales majeures - qui s'inscrit, du reste, dans un contexte beaucoup plus global de crise protéiforme – conduit à considérer comme possible, voire probable, l'hypothèse de futurs engagements des armées françaises dans des conflits de haute intensité s'inscrivant dans la durée.

Il importe donc, dès à présent, d'être prêts à ne pas subir en développant les capacités de résilience de la Nation et en veillant plus particulièrement à fournir à nos forces, dans les meilleurs délais, tous les moyens nécessaires leur permettant de conduire, avec succès, de tels engagements. C'est dans cet esprit que le ministre des Armées a lancé une réflexion sur le concept d'« économie de guerre » en y associant notamment l'état-major des armées, la direction générale de l'armement et les industriels de la défense.

La table ronde organisée à cet effet, le 7 septembre dernier, a déjà permis d'en préciser les grandes lignes dont l'identification des systèmes d'armes considérés à court terme comme les plus indispensables, l'adaptation de la conduite des opérations d'armement afin de les rendre plus réactives tout en les simplifiant, la sécurisation des approvisionnements et la constitution des stocks nécessaires.

Cette stratégie comporte logiquement une dimension sécuritaire au sein de laquelle la DRSD joue un rôle de premier plan en tant que « service de renseignement dont dispose le ministre de la défense pour assumer ses responsabilités en matière de sécurité du personnel, des informations, du matériel et des installations sensibles » comme le rappelle le Code de la défense.

Tout en s'adaptant en permanence à des évolutions de contexte qui se révèlent rapides, la DRSD entend donc poursuivre les missions de renseignement, de protection, de conseil et de sensibilisation qu'elle mène déjà depuis de nombreuses années au profit de l'ensemble des acteurs de la base industrielle et technologique de défense (BITD) qu'il s'agisse des maîtres d'œuvre industriels, des chaînes de sous-traitance ou encore des établissements de recherche associés.

Elle veillera notamment à identifier, voire à anticiper, les nouvelles menaces et vulnérabilités pouvant émerger et auxquelles il s'agira de faire face sans délai. À titre d'exemple, et comme l'a souligné le Ministre des armées, au-delà des multiples ingérences désormais considérées comme classiques, la résilience des outils de production face à de possibles actions de sabotage, tant physique que cybernétique, constitue, plus que jamais, un des enjeux majeurs. Dans un autre registre, il apparaît également crucial d'intégrer les ingérences se manifestant dans un espace informationnel devenu un champ de bataille à part entière.

Enfin, parce que le concept d' « économie de guerre » ne peut, par essence même, que s'inscrire dans une stratégie globale de défense et de sécurité nationale, la DRSD continuera d'apporter une attention particulière à la cohérence de son action au travers d'une coordination permanente avec ses partenaires publics au sein des différents ministères concernés et, naturellement, au niveau interministériel. Tel sera également le cas avec l'ensemble de ses partenaires privés au sein de la BITD, notamment au travers d'échanges permanents avec les chaînes de sécurité – sûreté dont ils disposent.

Dans un contexte aussi singulier qu'incertain, cette lettre d'information économique spéciale a vocation à vous proposer un éclairage sur certains enjeux majeurs liés à ce changement de paradigme.

Bonne lecture.

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

La DRSD au rendez-vous de l'économie de guerre

« 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 », la DRSD est pleinement investie dans le volet sécuritaire de la manœuvre ministérielle globale visant à répondre aux besoins du contexte d'économie de guerre (résilience des moyens de production, accroissement des acheminements et consolidation de stocks de matériels).

Dans ce cadre, si les menaces de sabotage sur la gestion des acheminements et les outils de production ressurgissent, y compris dans l'espace cybernétique, les autres menaces (terrorisme, espionnage, subversion, criminalité organisée) n'en demeurent pas moins réelles.

Concernant l'espionnage industriel, commercial et technologique, la DRSD constate en effet la persistance d'ingérences de plus en plus décomplexées (vols d'information et de supports numériques, prédation financière, ingérences juridiques etc.) qui s'attaque tant aux savoir-faire industriels qu'aux savoirs académiques et aux expertises technologiques nationales.

Par ailleurs, force est de constater que les conflits actuels donnent lieu à de véritables affrontements informationnels cherchant à influer sur les champs de perception, les prises de décision et les activités au travers d'actions de dénigrement et de manipulation. Dans ce domaine, la DRSD s'engage également, de manière résolue, aux côtés des acteurs nationaux publics et privés.

Les situations de pénuries en ressources stratégiques sont également susceptibles de favoriser des actes de délinquance, et notamment d'atteintes aux biens, y compris au sein de la BITD.

Enfin, de manière à pouvoir réaliser des analyses de risques et concourir à leur réduction, l'action de la DRSD porte également sur la détection et l'identification des vulnérabilités par le biais de ses prérogatives spécifiques en matière de contrôle, d'inspection, de conseil et de sensibilisation de l'ensemble de ses partenaires de la BITD.

Économie de guerre et espionnage industriel : un risque renforcé

Déjà vivace en temps de paix, l'espionnage industriel, technologique et commercial, s'accroît en temps de crise. En effet, la bascule d'une situation de compétition à une situation de contestation dans laquelle s'inscrit la mise en œuvre d'une économie de guerre ne fait pas disparaître les menaces d'espionnage. Elle peut, bien au contraire, renforcer la détermination des auteurs de ces menaces, voire en faire émerger de nouveaux.

La captation des savoirs et savoir-faire des industriels et établissements de recherche peut s'inscrire dans la poursuite de plusieurs objectifs.

Il peut tout d'abord s'agir d'obtenir des informations sur les capacités militaires auxquelles on peut être confronté. L'intérêt de la Russie pour les livraisons d'équipements à l'Ukraine s'inscrit dans ce cadre.

L'espionnage industriel et technologique contribue aussi à combler des lacunes technologiques. La rupture de circuits commerciaux et de partenariats, les sanctions et les embargos créent des situations d'isolement et rendent plus complexe le maintien à niveau technologique de certains pays.

Enfin, les bases industrielles et technologiques de défense s'appuient sur un modèle économique reposant en grande partie sur les activités à l'export
Le passage à l'économie de guerre ne met pas un terme à la guerre économique. Au contraire, la compétition s'intensifiant pour satisfaire des besoins accrus, voire nouveaux, en équipements, les rivalités concurrentielles peuvent avoir tendance à s'exacerber pour la conquête des marchés.

Les modes opératoires, qu'ils s'appuient sur des vecteurs humains et/ou techniques, sont déjà bien identifiés pour la plupart et demeurent pleinement d'actualité : intrusions consenties (salariés malveillants, stagiaires et acteurs non permanents, délégations de visiteurs), sollicitations extérieures (prise de contacts sur les réseaux sociaux comme LinkedIn, propositions d'entretiens rémunérés), vols de supports informatiques ciblés ou de matériels et matières premières, attaques cybernétiques.

Recommandations de la DRSD

- Apporter une vigilance accrue à la multiplication des incidents de différente nature, y compris dans les chaînes d'approvisionnement.
- Identifier précisément les informations et savoir-faire à protéger afin de concentrer les efforts de protection.
- Actualiser et tester régulièrement les dispositifs de protection existants.
- Etudier la mise en place de dispositifs récents tels que celui lié à la protection du potentiel scientifique et technique de la Nation (mise en place de zones à régime restrictif).

Intrusions et sabotage : la nécessaire sanctuarisation des sites de la BITD

Sanctuarisez vos sites afin de protéger les personnes, les biens, les savoir-faire.

L'ensemble des sites liés à vos activités (recherche & développement, production, logistique etc) peut susciter l'intérêt et la convoitise de nombreux acteurs (concurrents, groupes criminels, etc.) de tous ordres, du délinquant local au groupe étatique étranger, en passant par le mouvement subversif opposé au commerce de l'armement.

Certains peuvent tenter de s'approprier tout ou partie de votre production (vol de matières premières, de technologies, d'outils de production etc.) ou simplement de la retarder voire de l'empêcher en y portant atteinte au travers d'actes de sabotage.

Penser la protection de ses sites, c'est donc réduire les risques d'atteinte à votre production.

Recommandations de la DRSD

Une protection physique…

- Considérer les vulnérabilités de vos sites et les réduire par cercles concentriques (des zones les plus sensibles aux zones les plus périphériques) à l'aune des risques potentiels.
- Distinguer les zones accessibles au public (visites de délégations, prestataires extérieurs etc.), de celles réservées au personnel et s'assurer de l'herméticité de ces zones.
- Renforcer les contrôles de sécurité et de sûreté sur vos sites comme la protection des lieux de manipulation et de stockage des composants essentiels à la production.
- Se rapprocher des forces de sécurité intérieure afin d'être identifié et de développer des partenariats dans la gestion des incidents.
- Mettre à jour son corpus réglementaire de protection, qu'il s'agisse de l'analyse des risques « sécurité-sûreté », des plans de protection (plans de sécurité opérateur, plans particuliers de protection, plans de protection extérieure) ou encore des plans de continuité et de reprise d'activité.

… qui s'appuie sur un personnel formé et sensibilisé.

- Mettre à jour, optimiser, voire former et entraîner une cellule de gestion de crise où chacun connaît son rôle et ses interlocuteurs.
- Réaliser des exercices réels afin de tester les mesures de protection passive (contrôle d'accès, détection intrusion, vidéosurveillance) et la réactivité de la protection dynamique.
- Sensibiliser le personnel afin d'accroître sa vigilance, de développer sa capacité d'étonnement et son souci du compte rendu précis et rapide.
- Consolider les processus de contrôle au recrutement, en particulier lors de l'embauche d'intérimaires. Accorder une vigilance toute particulière à la détection des fausses identités.

Économie de guerre et exportations : les risques liés à l'intermédiation

Le passage à l'économie de guerre n'implique pas une allocation exclusive de toutes les capacités de production au profit des seules armées françaises. En effet, les exportations de matériels de guerre demeurent indispensables pour soutenir les pays alliés, mais également pour garantir la pérennité de l'outil national de production. La crise ukrainienne a créé des besoins d'équipement importants, et parfois nouveaux. Dans ce contexte, le contrôle des exportations assuré par l'Etat reste primordial, notamment pour éviter tout risque lié aux phénomènes non contrôlés d'intermédiation.

Depuis le début du conflit russo-ukrainien, beaucoup d'entreprises françaises ont sollicité l'autorisation d'exporter des matériels de guerre vers l'Ukraine. Un grand nombre de ces opérations d'exportations faisaient suite à des approches d'individus, français ou étrangers, se présentant comme intermédiaires travaillant au profit de sociétés ukrainiennes, voire de l'État ukrainien lui-même. Ce type de pratiques commerciales implique une vigilance particulière.

En effet, tout ressortissant français doit être autorisé pour intervenir dans des opérations de commerce ou d'intermédiation d'armement. *A fortiori,* tout étranger non connu de l'industriel doit faire l'objet d'une vigilance accrue. En cas de doute, la DRSD peut conseiller l'entreprise. Attirés par des opportunités financières, des escrocs peuvent en effet profiter du contexte actuel. Ces acteurs malveillants peuvent, en outre, favoriser des risques de trafic, de dissémination ou de détournement.

Les règles du contrôle des exportations de matériel de guerre demeurent donc plus que jamais en vigueur.
Le dispositif de contrôle repose sur un principe général de prohibition et de dérogation, qui induit le contrôle par l'État de l'ensemble du secteur de la défense et de ses flux.

Pour exporter du matériel de guerre, deux principes s'appliquent :

- être autorisé à commercer, voire à fabriquer (détenir une AFCI) ;
- demander à l'État une licence d'exportation.

Le délai de traitement d'une demande de licence d'exportation est d'environ quarante jours. Le traitement d'une demande peut être facilité grâce à la rédaction claire et précise de celle-ci, notamment en ce qui concerne le contexte de l'opération commerciale.

Les matériels de guerre A2 sont ceux listés à l'article R311-2 du code de la sécurité intérieure. La catégorie A2 se décline en 18 paragraphes : du A2§1° au A2§18°. À chaque paragraphe correspond une catégorie de matériel (avions, navires, blindés etc.). Le demandeur ne pourra exporter que du matériel pour lequel il est autorisé. Cette classification est nationale. Toutefois, l'Union européenne a adopté une liste de matériels qui englobe la catégorie A2 française, ainsi que d'autres matériels dits « assimilés » qui, classés à l'exportation, nécessitent une licence. Ils sont décrits dans la *Military List (ML)* de l'UE, disponible sur Internet.

La catégorisation du matériel exporté est de la responsabilité de la société exportatrice. En cas de doute, l'entreprise peut s'adresser à l'autorité nationale de classement, la Direction générale de l'armement (DGA/DI) : dga-di.classement.fct@intradef.gouv.fr. Pour davantage d'informations concernant l'exportation, les entreprises sont invitées à consulter le portail de l'armement de la DGA : www.ixarm.com.

Recommandations de la DRSD

- Accorder une attention particulière au classement des matériels potentiellement classés « de guerre » amenés à être exportés par l'entreprise, en relation avec l'autorité nationale de classement : la DGA/DI.
- Identifier toute approche d'entreprise à but d'information ou de demande d'acquisition par des individus, français ou étrangers, se présentant comme intermédiaires d'une société voire d'un État. Demander systématiquement une pièce d'identité et une lettre d'intention commerciale à ces intermédiaires. En cas de doute, un signalement peut être fait à la DRSD.

Risques cybernétiques et SSI « de guerre »

La dépendance du tissu économique au numérique a facilité la multiplication de nouveaux risques trouvant leur origine dans le cyberespace. La crise sanitaire a encore accéléré cette tendance, à travers l'adoption de nouveaux modes de travail.

Ainsi la porosité entre les systèmes d'information (SI) professionnels et les connexions privées depuis le domicile a engendré une augmentation de la surface d'exposition des entreprises aux attaques. Aujourd'hui, la cybersécurité fait face à un nouveau défi.

Dans le cadre des tensions internationales actuelles, des cyberattaques peuvent affecter les entreprises françaises, en particulier les capacités industrielles de production et de soutien, d'une part en ciblant les SI industriels, d'autre part en instrumentalisant la chaîne de sous-traitance en procédant à des attaques par rebond.

En effet, les entreprises disposent de systèmes SCADA isolés physiquement des autres SI par un réseau dédié et logiquement par des protocoles de communication spécifiques voire propriétaires. Ce cloisonnement pouvait apparaître comme une protection face aux problématiques cybernétiques mais l'augmentation de la connectivité a fragilisé ce rempart. Ainsi, les automates peuvent communiquer avec des protocoles en Ethernet (IP) ou s'interfacer avec les autres SI de l'entreprise (ERP, SIG). Exposés aux vulnérabilités informatiques, les systèmes SCADA sont essentiellement la cible de sabotage.

Pour autant, si l'entreprise peut être directement victime de cyberattaques par voie directe, les possibilités d'attaques via les chaînes de sous-traitance ne doivent pas être négligées. En effet, la volonté de sécuriser l'approvisionnement de ressources critiques peut conduire à la diversification des prestataires, la recherche de nouveaux fournisseurs ou encore au recours à des procédures rapides propres au temps de crise. Néanmoins, cette sécurité d'approvisionnement ne doit pas prévaloir sur la sécurité des échanges informatiques avec les partenaires, anciens et nouveaux, au risque d'exposer les SI de l'entreprise à des attaques par rebond.

Cela consiste pour l'assaillant à utiliser un ou plusieurs systèmes intermédiaires, qui vont participer à leur insu à l'attaque, afin de dissimuler son identité. Dans ce cas, la confrontation avec la victime ciblée n'est pas frontale : l'attaquant se concentre sur l'écosystème de sous-traitants ou de fournisseurs de services connectés aux SI de la victime pour exploiter d'éventuelles failles de sécurité. Les objectifs peuvent être le sabotage ou l'espionnage par l'exfiltration de données.
La vigilance devra donc être accrue concernant la menace de cybersabotage et cyberespionnage pouvant s'exercer sur les SI industriels de production (SCADA) et sur les chaînes d'approvisionnement de la BITD.

Recommandations de la DRSD

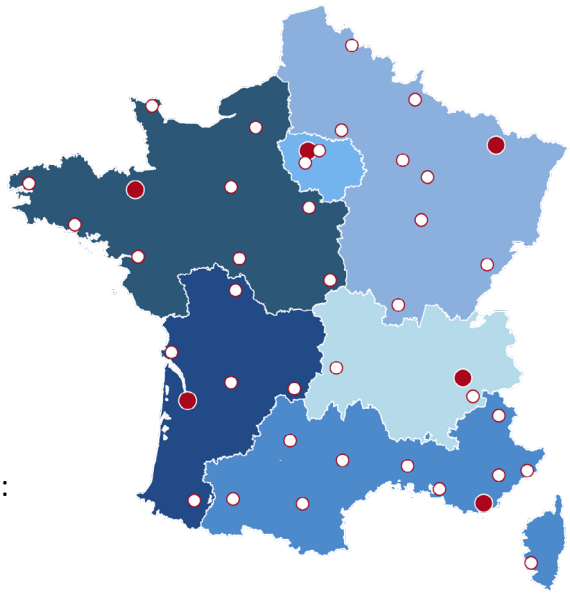
- Identifier les données stockées sur des serveurs à l'étranger, en particulier ceux situés en Europe de l'Est et caractériser leur sensibilité en vue d'un éventuel rapatriement.
- Contrôler les processus SSI, les amender si nécessaire (ex. segmentation de vos SI, contrôle des accès individualisé, processus de sauvegarde physique hors réseau etc.).
- Mener des investigations sur tout comportement SSI anormal (connexions inconnues, changement de mot de passe non sollicité, comportement anormal dans les logs) ou une tentative de cyberattaque.
- Alerter immédiatement en cas de contact cyber suspect (email, approche sur les réseaux sociaux etc.).

N'hésitez pas à contacter votre chaîne de sûreté/ sécurité au sein de votre établissement et votre agent DRSD référent afin de faire remonter toute ingérence ou atteinte (physique, économique, juridique, cybernétique, etc.) dont vous penseriez être victimes.
Soyez assurés que la DRSD et chacun des agents présents à votre contact sont présents à vos côtés dans ce contexte particulier.

Gardons contact

Direction Centrale, section « Sensibilisation » :
drsd-cie-sensibilisation.contact.fct@intradef.gouv.fr

Directions Zonales Ile-de-France :
Entreprises : **drsd-dsezp-4.cds.fct@intradef.gouv.fr**
Instituts et écoles de recherche : **drsd-idf.cmi.fct@intradef.gouv.fr**



Direction Zonale Nord-Est (entreprises et monde de la recherche) :
drsd-metz.cmi.fct@intradef.gouv.fr

Direction Zonale Ouest (entreprises et monde la recherche) :
drsd-rennes.cmi.fct@intradef.gouv.fr

Direction Zonale Sud-Est (entreprises et monde de la recherche) :
drsd-lyon.cmi.fct@intradef.gouv.fr

Direction Zonale Sud-Ouest (entreprises et monde de la recherche) :
drsd-bordeaux.cmi.fct@intradef.gouv.fr

Direction Zonale Sud (entreprises et monde de la recherche) :
drsd-toulon.cmi.fct@intradef.gouv.fr

Restons en contact