L'économie de guerre et l'incontournable résilience cyber de la BITD

Jean-Marie DUQUESNE
Général (2S)
Délégué Général
GICAT

Le GICAT (Groupement des Industries françaises de Défense et de Sécurité terrestres et aéroterrestres) est composé de plus de 450 adhérents, dont 78% de PME. Ses missions sont de porter leur voix, de les accompagner dans leurs stratégies à l'export, de leur apporter des informations stratégiques et de renforcer leur visibilité tout en facilitant les coopérations industrielles et l'innovation.

Le GICAT est un acteur clé du triptyque :
- Expression des besoins par les forces,
- Spécification du besoin et acquisition des capacités correspondantes par la Direction Général de l'Armement (DGA),
- Développement des solutions par les industriels de la défense.

En juin 2022, lors de l'inauguration d'Eurosatory, premier salon mondial de la Défense et de la Sécurité terrestres et aéroterrestres, organisé par le COGES Events, notre filiale commerciale, le Président de la République, Emmanuel Macron, déclarait **notre entrée en « économie de guerre »**. Cette volonté s'est concrétisée par une réelle impulsion et montée en cadence pour les industries de la Base Industrielle et Technologique de Défense (BITD) après plusieurs décennies de réduction liée aux dividendes de la paix. Dans le contexte géopolitique actuel, l'ensemble de la BITD a dû s'engager dans la préparation à un éventuel engagement majeur et se tenir prêt à produire plus vite et en plus grande quantité, constituer des stocks, **être résilient à tout type de menace, au premier rang desquelles figure la menace cyber**. Portés par cette dynamique, des groupes de travail au niveau du Conseil des Industries de Défense françaises (CIDEF) composé du GICAT, du GICAN et du GIFAS se sont constitués afin d'évaluer l'effort à consentir pour la mise en place de cette économie de guerre, aussi bien dans les champs matériels qu'immatériels dont celui de la cybersécurité, domaine transverse et désormais omniprésent.

A l'image des adhérents du GICAT, **les sociétés qui composent la BITD sont majoritairement des PME**. La sécurité de leurs systèmes et de leurs productions incombe souvent au chef d'entreprise, au même titre que de nombreuses autres activités et priorités. Or, **se « cybersécuriser » demande une expertise, du temps, des financements et un plan d'amélioration continu pour répondre à l'évolution permanente des menaces.** Le ministère des Armées a demandé à la DGA de mettre en place un Diagnostic Cyber Défense à la disposition des PME stratégiques de la BITD. Ce diagnostic, co-financé par BPI France, avait pour but d'inciter les industries à

évaluer leur niveau de maturité cyber et conduire les actions qui en découlent.

Au vu de l'enjeu et afin d'accélérer le processus, une logique un peu plus incitative a été adoptée. Dans le cadre de l'application de la convention cyber signée en 2019 entre les industriels et le ministère des Armées, la DGA, en concertation avec les grands maîtres d'œuvre, a souhaité mettre en place un référentiel de maturité cyber (RMC) dont le premier niveau dit « fondamental » a été présenté à l'ensemble de la BITD le 27 octobre 2023 lors d'un événement organisé à Balard avec la participation du GICAT, du GICAN et du GIFAS. La logique de ce référentiel est la suivante : toute société et ses sous-traitants qui ne seront pas en mesure de remplir les critères minimums du RMC se verront écartées des appels d'offres du ministère des Armées.

Se posent néanmoins plusieurs questions quant à la mise en place contractuelle de ce référentiel et à ses conséquences : **quelles en seront les obligations et quel sera le calendrier de mise en place de ces obligations ?** A titre d'exemple et de comparaison, pour l'environnement assurantiel et financier, le règlement DORA a précisé les actions obligatoires à mettre en place et donné 18 mois à l'ensemble des acteurs de la filière à laquelle cette norme s'applique pour se mettre en conformité. Aussi, si un projet de clause cyber a été présenté en mars 2024, **le volet contractualisation et ses modalités d'application n'est à ce jour pas arrêté**. Le titulaire aurait à sa charge la preuve de la conformité cyber de chacun de ses sous-traitants et les sociétés qui travailleraient dans la chaine de sous-traitance de plusieurs maîtres d'œuvre industriels se verraient contraintes de suivre le même processus autant de fois qu'il y a de maitres d'œuvres.

Se pose aussi la question de l'évolution de la norme : en parallèle du RMC, **la règlementation européenne NIS 2 devra être transposée dans le droit national à compter du mois d'octobre 2024**.

Si la DGA a présenté le RMC comme une première marche vers la conformité NIS 2 et un outil d'équivalence et d'harmonisation avec les textes existants en Europe, en Grande-Bretagne et aux Etats-Unis, **la crainte de la surtransposition** de cette directive et de la **multiplication de textes et autres référentiels demeure**. Face à la prolifération des normes et exigences, les plus petites structures vont faire face à **des coûts de mise en conformité très importants**. Il est par conséquent primordial **que l'acheteur final tienne compte de l'ensemble de ces nouveaux surcoûts dans les commandes futures.**

Dans ce contexte, l'ANSSI a effectué en fin d'année 2023 une consultation en trois phases auprès des groupements et fédérations, dont le GICAT, pour assurer la meilleure transposition possible de ces normes dans une logique sectorielle. Lors de cette consultation, ont été remontées des **demandes d'allongement de délais pour la mise en conformité** et une **application progressive** des exigences NIS 2 qui doivent être transposées et donc, appliquées en droit français à l'automne 2024. Une certaine souplesse a été confirmée par le Directeur Général de l'ANSSI, Monsieur Vincent Strubel, lors du Forum In Cyber qui s'est tenu en mars 2024, à Lille.

Il n'en reste pas moins que pour des PME, **le besoin d'accompagnement et de clarté des acteurs de référence est fort**, d'autant que NIS 2 a vocation à étendre son application à beaucoup plus d'entités régulées que le texte précédent (NIS 1). Certaines inquiétudes sont également remontées aussi bien sur **le niveau d'accompagnement financier auquel pourront prétendre les entreprises de la BITD** que sur **les sanctions en cas de non mise en conformité dans les délais imposés**. De plus, se pose la question de l'application de NIS 2 pour les entreprises de la BITD exerçant des activités duales (civiles et militaires) et son articulation avec d'autres textes tels que la directive sur la Résilience des Entités Critiques, ou encore le Cyber Resilience Act européen.

En conclusion, pour que la norme soit vertueuse, il faut qu'elle soit **claire, lisible et préparée dans l'anticipation et la concertation** avec les acteurs concernés et ce d'autant plus pour un secteur aussi stratégique que celui de l'industrie de défense et de sécurité. Cette norme doit être **adaptée à la taille des entreprises qui composent la BITD et les coûts induits doivent être raisonnables pour ce type de structures. Aussi, elle doit être accompagnée d'une aide opérationnelle en plus d'une aide financière.**

Pour la BITD, **l'ensemble de ces surcoûts en équipement de solutions cyber doit être accompagné et privilégié** par rapport au simple diagnostic.

Afin de répondre aux futurs niveaux du RMC, il vaut mieux concentrer le financement public vers l'équipement en solutions plutôt que vers de simples diagnostics dont on sait à ce jour qu'ils attesteront d'un niveau globalement insuffisant.

Enfin, en vue de la complexité des futures obligations des niveaux 1 à 4 du RMC, il serait intéressant de créer des labels ou des certificats permettant d'attester **que les prestataires de service sont qualifiés, souverains** (au vu de la sensibilité des données) et **disposent du niveau technique requis** par le RMC. Par ailleurs, il sera nécessaire de consolider cette base des partenaires de confiance et de définir les procédures de mise en relation avec les PME de la BITD.