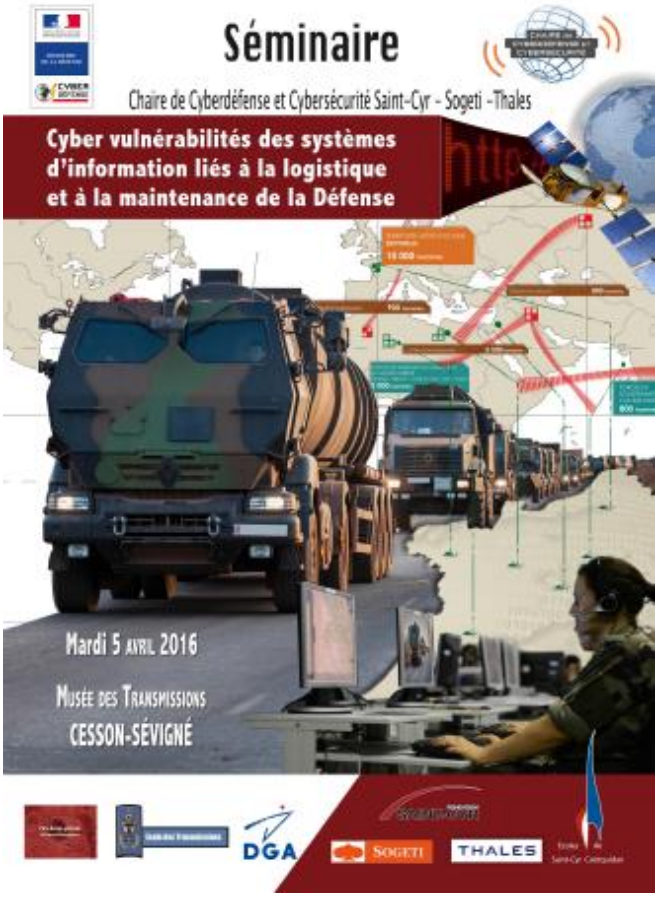
Cyber vulnérabilités des systèmes d'information liés à la logistique et à la maintenance de la Défense

mardi 5 avril 2016 – Musée des transmissions de Cesson-Sévigné



Compte-rendu

du séminaire de la chaire de cyberdéfense et cybersécurité Saint-Cyr – Sogeti – Thales

Présentation

La logistique et la maintenance ont un rôle central dans la conception et la conduite du soutien logistique en opérations extérieures, comme sur le territoire national. Elles regroupent le matériel de soutien de l'homme, de transport, de mise à disposition, d'approvisionnement, de dépannage et d'aide au déploiement des unités.

De nos jours, afin d'être plus efficients, on assiste à une utilisation accrue des systèmes d'information logistiques et de maintenance, qui permet une anticipation et une réactivité supérieures dans la planification et la conduite des opérations. Cette utilisation va de pair avec des échanges croissants d'informations avec les entreprises civiles vers qui ses fonctions de maintenance et de logistique ont été externalisées.

Or la « cyberconflictualité » qui constitue désormais une composante importante de la conflictualité en général, peut produire ses effets jusque dans ces systèmes et paralyser ou perturber leur bon fonctionnement. Il importe donc de prendre en compte les cybermenaces de la conception de ces systèmes à leur mise en œuvre opérationnelle au quotidien. Leur maîtrise revêt un enjeu crucial pour assurer une logistique et une maintenance efficace au profit de nos forces.

C'est l'un des défis qui s'annonce pour la logistique terrestre de demain, et c'est la raison pour laquelle – dans le prolongement des trois séminaires précédents – les écoles de Saint-Cyr Coëtquidan ont organisé le mardi 5 avril 2016 avec l'École des Transmissions et la DGA Maîtrise de l'information, dans le cadre des travaux de la chaire de cyberdéfense et cybersécurité Saint-Cyr – Sogeti – Thales, un nouveau séminaire portant sur les « cyber vulnérabilités des systèmes d'information liés à la logistique et à la maintenance de la Défense ». En voici le compte-rendu.

Glossaire

CCPA : Centre de cyberprotection des armées.

CEPIC : Commandement des programmes interarmées de cyberprotection

CSOA : Centre de soutien aux opérations et aux acheminements

CTTS : Centre de transport et transits en surface

CVSS : Common Vulnerability Scoring System

MCO : Maintien en conditions d'opération

MCS : Maintien en condition de sécurité

NEB : Numérisation de l'Espace de Bataille

RFID : Radio Frequency Identification

RSSI : Responsable de la sécurité des systèmes d'information

SIA : Système d'information des armées

SIAG : Systèmes d'information d'administration et de gestion

SIL : Systèmes d'information logistique

SILRIA : Système d'information logistique de suivi de la ressource interarmées

SIOC : Systèmes d'information opérationnelle et de commandement

STCIA : Socle technique commun interarmées

Introduction

Pendant la bataille de Verdun, en 1916, l'armée française a pu tenir le front grâce à la mise en place d'une gigantesque opération de logistique militaire visant à transporter le matériel et l'approvisionnement au front mais aussi à faire tourner les effectifs afin d'opposer aux Allemands les troupes les plus fraîches possibles. Cette opération est matérialisée par l'utilisation de la Voie sacrée, route reliant Bar-le-Duc à Verdun, axe stratégique vital qui a donné la possibilité de transporter par semaine un total de 90 000 hommes, de 50 000 tonnes de matériel en parcourant près d'un million de kilomètres tout en mobilisant 3 500 camions. Cet effort logistique a permis à la France de remporter une bataille décisive quant à l'issue de la Première Guerre mondiale.

C'est par cet exemple que l'ingénieure générale Marie-Noëlle SCLAFER souligne l'importance de la logistique, abordée sous l'angle cyber, dans la conduction d'une entreprise militaire. Parce qu'ils ne traitent pas d'informations opérationnelles, parce qu'ils interviennent en périphérie des systèmes d'arme, les systèmes logistiques sont souvent peu classifiés, peu visibles au sens sécuritaire alors même qu'ils sont indispensables à la bonne conduite des opérations militaires. Ces systèmes sont ouverts sur le monde extérieur, fortement interconnectés avec des systèmes très classifiés mais aussi avec l'univers anarchique du cyberespace. Or, c'est toujours le maillon le plus faible de la structure qui est la cible des attaquants ; le système d'information logistique devient donc une cible, surtout pour des attaquants opportunistes. Il ne s'agit pas d'aller contre le sens de l'évolution des technologies qu'elles soient relatives aux armes ou aux soutiens. Elles représentent des opportunités et permettent des gains considérables sur le terrain et sur le plan financier. Aussi, il est donc impératif de sécuriser ces évolutions afin d'en tirer le meilleur parti.

A – place de la logistique au sein de la NEB : importance des flux logistiques et de la maintenance au sein des missions du MINDEF

A.1 – Spécificité de la logistique militaire au travers de cas concrets

Dans sa présentation générale des spécificités de la logistique militaire, le colonel L'HOSTIS rappelle qu'historiquement, le monde militaire est *leader* dans le domaine de la logistique. Dès le XIX^{ème} siècle, le baron Antoine de Jomini, contemporain de Carl von Clausewitz, fait le lien entre la logistique et la tactique. Selon lui, la logistique est « l'art pratique de mouvoir les armées », le ravitaillement est donc nécessaire pour s'engager dans des conditions satisfaisantes. La logistique est assimilable au cordon ombilical : quand un commandement parvient à faire tourner les effectifs à Verdun, quand l'effort est porté sur l'artillerie car elle dispose d'obus en quantité et en qualité aux pieds des pièces, quand l'armée française résiste dix mois grâce à la Voie sacrée, il est aisé de prendre toute la mesure de l'importance de la logistique ; c'est ce qu'illustre la bataille de Verdun en 1916 avec la voie sacrée. Dans l'Histoire, cette spécificité de la logistique militaire s'est illustrée lors du débarquement du 6 juin 1944. Nous oublions assez souvent que l'opération logistique débute dès les plages et que l'acheminement des munitions, du carburant et de tous les moyens nécessaires, dans ce contexte, relève de l'exploit, d'autant plus que les militaires de l'époque ne disposaient pas de systèmes d'information tels qu'aujourd'hui. Le général Dwight Eisenhower disait en 1944 : « Il n'y a pas de tactique sans logistique. Si la logistique dit non, c'est qu'elle a raison » et son contemporain Somerwell ajoutait : « La bonne logistique seule ne peut pas gagner de guerre. La mauvaise logistique seule peut en perdre une ».

Le colonel Philippe L'HOSTIS attire l'attention sur le fait que la généralisation du maintien de l'ordre effectué par nos armées en opération extérieure ces dernières années ont fait oublier l'importance de la logistique. À la fin des années 1950, le *leadership* du domaine logistique se déporte vers l'industrie civile avec l'apparition des nouvelles technologies et de l'informatique. Le militaire devient alors suiveur, même si, tirée par le civil, la logistique

militaire garde ses spécificités. Elle a une fonction de soutien de l'administration militaire (d'un point de vue administratif, juridique et financier) et de soutien dans le but de vivre, combattre, se déplacer (hygiène, sécurité, soutien médical, pétrolier, de l'homme, munitions, acheminement, protection de l'environnement, maintien en condition, en stationnement). Face à ces multiples domaines, les systèmes d'information sont un moyen de répondre à la demande dans un objectif de vision globale et de performance. Depuis, les armées sont entrées dans cette recherche de la performance avec l'objectif clair de construire une chaîne logistique (*supply chain*) pour gagner des postes, des effectifs ou des finances par exemple. Pour le logisticien, les notions de prévision, de gestion et de distribution sont très importantes et il s'agit pour lui de trouver le bon équilibre entre l'entreposage et la distribution. Mais, les réductions d'effectifs, de terrains impliquent la sollicitation du secteur privé dans les marchés globaux, ce qui peut engendrer des problèmes de sécurité. Dans l'organisation de la *supply chain*, la distribution représente une partie du travail de performance par l'accélération du flux logistique et le pilotage de la ressource lors de la logistique retour. Celle-ci consiste à faire revenir les rechanges réparables en métropole, à les réintégrer dans la chaîne industrielle pour les reconditionner. Dans l'organisation de la *supply chain*, ce point est capital et il est impératif de se montrer de plus en plus performant dans le domaine de la logistique retour. La distribution s'adapte à l'entreposage comme la logistique s'adapte à la tactique. Elle implique de faire parvenir sur le territoire nationale en quelques jours des ressources en qualité et en quantité ce à quoi les systèmes d'informations apportent une aide efficace.

Le Centre de transport et transits en surface (CTTS) met en œuvre les transports au niveau interarmées. Il organise les missions de transport national et régional et prend en compte la gestion des plate-formes de transit ainsi que des lignes régulières. Le Centre de soutien aux opérations et aux acheminements (CSOA) dispose de la tutelle fonctionnelle sur le CTTS, il s'occupe pour sa part de l'acheminement.

- Le transport est le déplacement d'une ressource sans opération de transit ou douanière. Autrement dit, c'est un déplacement en métropole sans changer de mode de transport (routier, aérien) d'un point A à un point B.
- L'acheminement est une combinaison de transports (changer de mode, opérations douanières).

S'en sont suivis les exemples des opérations SERVAL et KAPISA, donnés pour démontrer l'importance et la spécificité de la logistique militaire. La vulnérabilité des convois par exemple (*soft target*) qui sont en mouvement pendant plusieurs jours fait l'objet d'une prise en compte sérieuse. Le logisticien militaire se doit d'anticiper l'action, de comprendre la manœuvre tactique, de chercher à conserver de la stabilité pour que les acteurs logistiques puissent travailler. Le tacticien doit mettre le logisticien en capacité de pouvoir répondre au soutien dont il a besoin. En résumé, il ne faut jamais oublier que la logistique est le domaine où l'on doit être le plus vigilant car c'est une cible facile, vulnérable.

A.2 – Cyber vulnérabilité des systèmes existants et leur nécessaire prise en compte

Les systèmes d'information logistique (SIL) présentent globalement les mêmes vulnérabilités, que les systèmes d'information opérationnelle et de commandement (SIOC). Cependant, les vulnérabilités des SIL impactent de nombreux domaines. Le lieutenant-colonel Thierry KESSLER-RACHEL explique dans un premier temps le rôle du Centre de cyberprotection des armées (CCPA). Sous l'autorité du Chef d'État-Major des Armées (CEMA), il travaille à l'homologation des systèmes d'information, effectue des actions de contrôles et produit des synthèses de vues liées à la cyberdéfense. Le CCPA fait partie du Commandement des programmes interarmées de cyberprotection (CPIC) aux côtés du Centre interarmées pour l'administration et l'interopérabilité des SIOC (CIADIOS). Ce dernier établit différentes vues, modélise des processus, représente les systèmes d'information selon différents plans. Le plus connu, le plan d'occupation des sols, permet aux décideurs de visualiser où se situent les systèmes d'information et comment ils interagissent entre eux. Les systèmes d'information d'administration et de gestion (SIAG) et les SIOC sont regroupés par zones fonctionnelles. La zone fonctionnelle logistique est placée sous l'autorité d'un responsable qui prend toutes les décisions relatives aux projets liés aux SIL. La zone fonctionnelle logistique est elle-même découpée en quartiers fonctionnels qui correspondent aux différents types de matériels (terrestres, aéronautiques, navals, santé, etc.). L'objectif du CIADIOS est de rationaliser l'ensemble des systèmes d'information pour, par exemple, empêcher les doublons. Il s'agit aussi de formaliser les métiers des armées sous la forme de processus, de procédures de maintien en conditions d'opération (MCO) en découpant les

opérations pour engager une automatisation et mieux écrire le cahier des charges. Tout ce développement est utile pour la compréhension de l'impact de l'exploitation des vulnérabilités sur les systèmes d'information.

Le responsable de la zone fonctionnelle logistique rappelle que les SIL doivent être sécurisés et les projets pilotés. La zone fonctionnelle logistique est fortement adhérente d'autres domaines (les ressources humaines, la santé, les finances). Les SIL sont sujets aux vulnérabilités habituelles des SIOC mais ils peuvent cependant être mis en relief. Ils sont interconnectés avec de nombreux éléments comme les systèmes d'arme ou les systèmes partenaires externes. Les SIL sont de plus étudiés de manière différente des SIOC. Les canons habituels de l'analyse de risque concernant les SIOC mettent en avant la confidentialité. D'ailleurs, des réseaux sécurisés sont spécialement conçus pour cela. Les SIL, parce que fortement interconnectés, parce qu'ils irriguent de nombreux métiers ne sont en général pas classés confidentiel-défense mais diffusion restreinte. La disponibilité des SIL, cependant, revêt une importance capitale alors que les SIOC s'appuient sur des réseaux support globalement disponibles (comme le réseau satellitaire par exemple). L'intégrité, dans les deux cas, est traitée de la même manière.

L'exploitation des cyber vulnérabilités a un impact fonctionnel sur l'intégrité et la disponibilité directe des systèmes d'arme avec pour effet des dommages collatéraux vers les partenaires financiers ou industriels, sur l'acheminement du matériel ou encore sur l'image de marque de l'institution qui se trouve mise à mal. La vulnérabilité des systèmes d'information est habituellement découpée en plusieurs causes possibles :

- **Gouvernance emploi-projet.** S'il n'y a pas d'autorité d'emploi, de responsable de la sécurité des systèmes d'information (RSSI) dans le cas de systèmes obsolètes par exemple, il ne peut y avoir de direction assurée. Sans gouvernance ni structure de projet, il n'y a pas d'administrateur. Cette vulnérabilité empêche l'application globale des corrections et des mises à jour.
- **Parc hétérogène des systèmes d'information.** Cela implique de nombreuses formations différentes, de nombreux personnels et des problèmes d'obsolescence logicielle et matérielle.

- **Maintien en condition de sécurité (MCS).** La mise en œuvre du MCS reste un processus généralement complexe.
- **Défaut de configuration système ou réseau support.** Cette vulnérabilité est liée au non-respect des règles de sécurité par l'utilisateur qui ne se réfère pas aux guides.
- **Réseau support.** Lui-même peut présenter des vulnérabilités et ses extensions de même.
- **Technicité accrue des systèmes d'information.** Une administration compliquée qui doit être prise en charge par l'industriel lui-même.

Pallier à ces failles n'est pas chose aisée. Il faut d'abord connaître précisément ce qu'il y a à défendre pour ensuite comprendre l'impact d'une attaque sur le système. Il faut aussi pratiquer l'homologation, allouer des finances et sensibiliser la hiérarchie sur les risques et les protections liés à l'utilisation du système. Pour cela, il est possible de mettre en place une gestion des risques possibles et il convient de nommer un RSSI. Comme moyen de détection des menaces, nous sommes en mesure d'installer des sondes. Il est aussi possible de réduire la surface d'attaque, de revenir à une moindre sophistication mais cela empêcherait d'utiliser les fonctionnalités et les gains que permettent les évolutions technologiques. Pour faire face à un incident sur un temps donné, travailler en mode dégradé peut être une solution à court terme (fax, transport), tout comme le recours au réserviste – si tant est qu'il soit bien formé pour être apte à réagir – ou l'établissement d'un plan de continuité d'activité. Pour résumer, connaître ce qu'il y a à défendre implique d'effectuer de nécessaires travaux de cartographie des systèmes pour ensuite pouvoir faire connaître les risques et engager des plans de réaction pour les réduire.

B – La prise en compte des vulnérabilités

B.1 – Prise en compte de la sécurité dans les systèmes logistiques : les exigences dans leur définition et dans l'administration/contrôle des systèmes

Lors de cette intervention, Monsieur Michel VIEILLARD a particulièrement souligné l'importance d'intégrer les systèmes d'information dans une approche globale de la sécurité. En effet, la sécurisation des systèmes d'information et des systèmes d'arme s'est le plus souvent cantonné à la protection des informations et la dimension disponibilité s'est traduite par une prise en compte moindre du réflexe sécuritaire sous prétexte que les systèmes de maintenance ne véhiculeraient pas d'information sensible. Mais, désormais, comme tout est de plus en plus interconnecté, les nouvelles technologies rendent difficile la sécurisation des systèmes de défense, des systèmes d'information opérationnelle, des systèmes d'information logistique et des systèmes d'arme, des systèmes industriels, d'infrastructures et de servitudes. La notion de sécurité globale est d'importance capitale ; par exemple, sur un avion, le système d'arme, les systèmes de soutien et tous les autres vont être interconnectés et sans prise en compte de la sécurisation de toutes ces interconnections, cet avion peut rester cloué au sol. Pour rappel, la sécurité concerne un risque provenant de l'environnement et dont les conséquences potentielles concernent le système alors que la sûreté concerne un risque provenant du système et dont les conséquences potentielles concernent l'environnement. Concrètement, l'acte malveillant relève de la sécurité, l'accident, lui, relève de la sûreté selon le modèle défini dans la thèse de Ludovic Piètre-Cambacédès sur les relations entre sûreté et sécurité.

On constate une dématérialisation et une numérisation des échanges, une utilisation de produits informatiques sur étagère[1] ce qui crée d'autant plus de failles cybernétiques. L'aspect MCS est lui aussi jugé très important ; il est possible de livrer un produit (un système) très

[1] Se dit d'un produit fabriqué en série et non spécifiquement pour un projet. Ils sont utilisés pour réduire les coûts de conception, de fabrication et de maintenance.

fiable et très efficient contre les attaques déjà connues mais si dans le temps le MCS n'est pas implémenté et suivi, le produit (le système) peut devenir vulnérable. Or, on constate une numérisation croissante des systèmes d'arme doublée d'une contrainte très forte sur les effectifs opérationnels pour servir ses systèmes. Il s'en suit une externalisation croissante des systèmes de maintenance et de la maintenance de nos systèmes qui conduit à une multiplication des interconnections avec les industriels, favorisant l'apparition de nouvelles vulnérabilités si ces systèmes d'information sont raccordés à internet. La DGA étudie les risques pesant sur l'ensemble des systèmes, qu'ils soient d'arme, de soutien, d'information ou de maintenance à l'aune du principe de sécurité globale. Elle prend en compte la nécessité d'établir et de suivre un maintien en conditions de sécurité sous peine de voir le risque prendre de plus en plus d'importance. En effet, l'attaquant suit toutes les évolutions des systèmes de sécurité. Sans mises à jour, il risque de pouvoir pénétrer les systèmes.

Une solution de sécurisation des SIL consiste à les porter sur des systèmes déjà sécurisés, sur l'INTRADEF, l'INTRACED, le socle technique commun interarmées (STCIA). Dans tous les cas, la sécurisation des systèmes est donc une activité constante qui ne se fige pas dans le temps. Il faut donc prendre en compte l'ensemble des cycles de vie des systèmes et identifier les SIL comme des systèmes en interface avec les systèmes d'armes, interfaces qu'il faut ensuite sécuriser sous peine de les voir devenir le maillon faible du système. Au-delà des aspects protection, la priorité du pôle SSI est de prendre en compte la lutte informatique défensive (LID) sur les systèmes déployés afin d'avoir une vision permanente de l'état de sécurité du système.

L'industriel, lui, est potentiellement un maillon faible car ses plate-formes sont moins classifiées et l'attaquant peut facilement éprouver la sécurité de l'entreprise. Cela engendre l'exigence d'effectuer des analyses de sécurité et de risques pour connaître les menaces et leurs occurrences, savoir de quoi se protéger, l'impact sur les systèmes. Notons que la dimension coopérative est bien présente dans le développement de certains systèmes d'arme comme l'hélicoptère Tigre par exemple. De la même façon qu'il faut prendre en compte la présence d'éléments « spécial France » dans ces systèmes développés en coopération pour ce qui concerne le maintien en condition des équipements, il faut faire de même avec le MCS. Il est de plus impératif de prendre en compte l'ergonomie pour limiter les erreurs humaines car si la sécurité est trop contraignante, l'utilisateur contournera mes mécanismes de sécurité afin de

répondre aux exigences de sa profession (un militaire face à une situation d'urgence devra appliquer une réponse immédiate). Un autre risque concerne les impacts de la classification des matériels sur la logistique car ils peuvent engendrer de nouveaux circuits de maintenance très contraignants.

Pour conclure, la DGA prépare le futur, lance des travaux sur les nouvelles technologies et accompagne les forces pour maîtriser les risques cyber liés à ces nouveaux modes de fonctionnement. La sécurité doit être appréhendée de façon globale, sur toutes les phases du cycle de vie des systèmes et des mesures de protection doivent être imposées aux industriels. Enfin, des mesures de LID devront être mises en place sur l'ensemble des systèmes (sonde réseau ou de détection par exemple).

B.2 – L'exemple de l'armée de l'air dans la supervision des flux logistiques, la prise en compte des menaces et des mesures correctives (MCS)

Le commandant MARTIN et le commandant BUSTOS-SALIDAS s'attachent, au sein du Groupement aérien de l'informatique opérationnelle (GAIO), à exercer une ingénierie logicielle (développer des SIO au profit de l'armée de l'air), un appui aux opérations (administration et soutien aux systèmes essentiels pour les opérations aériennes, mise en œuvre et sécurisation des tablettes embarquées dans les avions) et des missions de cyberdéfense (MCS des SIL et SIOC, cyber surveillance, constitution d'un noyau dur d'intervention). Le MCS pour l'armée de l'air vise trois objectifs. a) Le premier consiste à connaître les limites de notre cyberespace. C'est un défi permanent car tous les jours apparaissent et disparaissent des applications ce qui rend les contours du cyberespace flous, mouvants, dynamiques. Être capable de cartographier les applications, les recenser et les décrire n'est certainement pas chose aisée et implique de savoir décrire ses éléments constitutifs, définir et identifier ses limites physiques et logiques, modéliser ses dépendances internes et externes. b) Le MCS permet, dans un second temps, d'établir un niveau de confiance acceptable, de l'évaluer, de définir le niveau de sûreté du système et de pouvoir en rendre compte. c) Troisièmement, il doit être capable de servir de base de connaissance en cas d'événement cyber, de définir l'impact opérationnel (et donc la perte de capacité), de confiner l'incident et ensuite d'éradiquer la menace pour retrouver un système sain. Plus le système

sera décrit qualitativement, quantitativement et géographiquement, plus la cyberdéfense pourra être efficace.

La mise en œuvre du MCS dans l'armée de l'air s'effectue grâce aux RSSI qui utilisent un système dédié créé par le GAIO ; PAVENSIS. Le MCS s'appuie aussi sur le Centre d'analyse de lutte informatique (CALID) qui transmet au GAIO les vulnérabilités connues et demande un traitement adéquat. Le GAIO prend à son compte le CVSS (*Common Vulnerability Scoring System* = niveau de criticité d'une vulnérabilité) et aide le RSSI dans ce calcul de criticité et dans l'élaboration d'une mesure de correction. Le MCS permet de maintenir le niveau de confiance du système jusqu'à la fin de son cycle de vie. Concernant spécifiquement les SIL, nous pouvons dire qu'ils sont vulnérables. Certains peuvent être obsolètes, car le cycle de vie d'un système d'information s'accommode mal au cycle de vie du matériel. Ils sont souvent isolés car trop dédiés, avec une forte adhérence avec le matériel. Néanmoins, l'ensemble des systèmes doivent travailler ensemble et des moyens d'échange sont mis en œuvre parfois même via USB, même si la mise l'interconnexion des systèmes progresse. On se retrouve donc avec des systèmes obsolètes engendrant des échanges nombreux. Si l'on rajoute que la maîtrise d'œuvre étatique n'est que partielle car confiée en partie aux industriels, on a une démultiplication des acteurs intervenants. Enfin, nous n'avons aucune visibilité sur les briques logicielles fournies par les industriels et l'état des composants fournis. Or pour intégrer les MCS dans la sécurité globale, il faut être capable de prévoir les délais de traitement, d'anticiper avec des procédures identifiées et intégrer, formaliser les tests de non-régression. Il faut par conséquent intégrer les industriels dans le processus de MCS. La menace est globale, la réponse doit être globale. Il faut pouvoir établir une grille d'exigences respectées par les industriels, lesquels doivent fournir les vulnérabilités inhérentes à leurs briques logicielles. L'armée de l'air a atteint un premier niveau de maturité en ce qui concerne le MCS, dont le GAIO est chargé. La prise de conscience du niveau de menace a permis d'armer des postes de responsables SSI formés et d'avoir une cartographie assez juste bien que toujours à compléter.

B.3 – L'OTAN : quelles réponses vis-à-vis des vulnérabilités dans la chaîne logistique de l'alliance ?

L'OTAN, présentée par le colonel Jean-Luc MERCADIER, dispose de logiciels (*logistic apps*) visant à gérer la logistique. Il existe dans l'OTAN deux réseaux, un dédié aux opérations (très sécurisé, classifié NATO SECRET) et un autre dédié au *business* (moins sécurisé, classifié NATO RESTRICTED ou NATO UNCLASSIFIED). La logistique est considérée comme relevant de l'opérationnel et elle reste donc très cloisonnée, rien n'étant accessible par internet. LogFAS (systèmes logistiques associés à l'aire fonctionnelle logistique) est une application parmi d'autres (ADAMS, EVE, CORSOM) qui soutient le pôle logistique de l'OTAN lequel couvre beaucoup d'aspects, notamment l'acheminement des moyens. Elle s'appuie sur une base de données commune qui peut être interconnectée avec l'extérieur. Ces modules logiciels sont intégrés à la planification de défense au même titre que la planification opérationnelle. À travers le système logistique ADAMS, le système de l'OTAN est connecté aux systèmes de déploiement nationaux ce qui implique de nombreuses interfaces (une par pays) et donc de nombreux points de vulnérabilité. Chacune des nations doit donc se mettre au niveau sécuritaire. A cet effet, la version future de la suite logicielle logistique s'appuiera sur une architecture de bus de service ce qui permet de rationaliser les interfaces et donc de mieux les protéger.

L'OTAN est un concept stratégique fondé sur trois piliers : collective defense (défense collective), crisis management (gestion des crises), cooperative security (sécurité coopérative). Depuis 2002, toutes les déclarations qui suivent un sommet de l'OTAN parlent de cyber. L'article 5 porte spécifiquement sur la défense collective et l'Alliance a, depuis le Wales summit de 2014, élevé au maximum le niveau de réaction à une attaque cyber. C'est-à-dire que la réaction collective à l'attaque cybernétique d'un pays membre est maintenant affirmée. L'OTAN ne découvre pas le sujet car une nation a déjà subi une attaque majeure : l'infrastructure de l'Estonie a par exemple été attaquée en 2004 et avait alors été défendue par l'Alliance. Par ailleurs, l'OTAN a mesuré l'impact militaire des attaques cybernétiques en observant la paralysie de l'infrastructure de commandement de la Géorgie lors de l'attaque russe en 2008. Pour faire face, l'OTAN a mis en place une politique de cyberdéfense qui se concentre seulement sur ses moyens propres (la structure de commandement) en laissant aux États le soin de gérer de manière souveraine la protection de leurs systèmes nationaux. La

posture cyber de l'OTAN, défensive seulement, s'adresse donc essentiellement aux SIC qui sont possédés et mis en œuvre par l'OTAN. L'Alliance protège aussi les extensions nationales car elles soutiennent le système de consultation des alliés qui est vital pour réagir en coalition.

On trouve le cyber dans tous les niveaux et notamment au Conseil de l'Atlantique Nord où se retrouvent les ministres de la Défense. Les deux commandements stratégiques de l'OTAN se partagent le spectre des capacités : l'ACT dirige la transformation de la structure, des forces, des capacités et de la doctrine militaires de l'OTAN et le Commandement allié Opérations (ACO), situé au SHAPE, est responsable de la planification et de l'exécution de toutes les opérations militaires de l'Alliance. Le SHAPE s'organise pour mettre en place un organisme de *cyber situational awarness* qui s'appuie sur une étude de la menace sur les systèmes, de l'état des réseaux et enfin de l'impact que ces menaces peuvent avoir sur l'opérationnel. Une *task force* cyber est dédiée à cette tâche. Le *Cyber as a domain* (cyber en qualité de domaine) vise à considérer le cyberespace comme un espace aérien, maritime, terrestre et spatial qui s'accompagne de la création d'une cyber-division au SHAPE. Cela donne au commandement opérationnel la possibilité de se coordonner avec les acteurs nationaux et, en cas de guerre, permet d'absorber les aspects légaux d'un conflit et donc de mettre en œuvre tout le spectre stratégique possible d'une réponse à un événement.

C – Les systèmes d'information logistiques d'aujourd'hui et de demain

C.1 – SIA : le futur système d'information des armées

Le système d'information des armées (SIA), lancé fin 2012, a été présenté par le lieutenant-colonel Samuel DUVAL et par monsieur Jacky TÉTAUD en tant que système englobant SILRIA. Le but est de prendre en compte la numérisation de l'espace des opérations en offrant une garantie globale de fonctionnement répondant aux besoins de tous les milieux. C'est le successeur unique de nombreux SIOC et en particulier des SIOC de milieux (SICF, SIC21, SCCOA). Il met en cohérence les SIOC participant et réalise, intègre certains sous-systèmes. Ce système, créé dans une logique de convergence, est basé sur le socle technique commun interarmées (STCIA). Le but est de dépasser la logique de milieu vers une logique de métier, le combat étant interarmées par nature et la logistique tout particulièrement. Les briques (SIAC2, SORIA, SILRIA) se poseront petit-à-petit pour s'emboîter sur le socle STCIA. Posé sur des socles techniques communs, différents services (annuaire, messagerie, gestion des documents, etc.) sont mis à disposition ainsi que tous les services de sécurité pour l'ensemble du système.

Le système d'information prend en compte la SSI de façon globale et cohérente pour se protéger avec un haut niveau de sécurité, d'intégrité, de disponibilité et de fiabilité. On s'appuie sur des socles (STCIA, STC E) pour amener les services de sécurité (GSYS, GSEC) pour l'ensemble du SIA sur l'intranet (INTRADEF, INTRACED). Pour assurer la soutenabilité de l'ensemble, les principes de MCO et de MCS seront appliqués. Les services fournis par le STCIA (référentiel documentaire, portail de travail collaboratif, communication instantanée) sont aussi de nature sécuritaire : OS sécurisé, contrôle d'intégrité, antivirus, contrôle d'accès, authentification unique, audit, accès nomade. Il faut également trouver un juste milieu entre la qualification du système et son déploiement afin d'avoir un emploi en conditions réelles acceptable. Les fonctions SSI essentielles mises en œuvre reposent en particulier sur une authentification très forte avec la mise en place de cartes à puce, de

certificats IGCNG, de deux systèmes d'authentification en série et enfin avec des authentifications via l'utilisation de macro-droits et de micro-droits. Il existe un cloisonnement des réseaux avec l'un dédié à l'administration technique (accès unique), intégrant une séparation physique avec les réseaux d'infrastructure et les réseaux d'exploitation et d'administration, et les postes utilisateurs. Les postes exploitants se trouvent sur des LAN dédiées. Au niveau des fonctions SSI principales, on met en œuvre des plans de continuité ou de reprise informatiques (PCI/PRI) pour assurer une grande disponibilité du système. Il existe aussi des fonctions de surveillance et de supervision de lutte informatique défensive (LID) au travers de la centralisation des logs avec l'application GSEC. Il existe également un outil de supervision technique et fonctionnelle centralisée (GSYS). L'intégrité du système est prise en compte au travers de solutions antivirales (sur les postes utilisateurs, serveurs, messagerie). Le dispositif de signature électronique est couplé à la messagerie officielle.

Notons que le défi de l'année 2016 est le passage du SIA sur le FROPS 2.0 qui fait suite au FROPS 1.0 déployé par la DIRISI, système qui permet d'effectuer des échanges au niveau national, bilatéral et interallié. Les développements du SIA intégrés sur le FROPS assureront la continuité des échanges de bout en bout entre la métropole et le théâtre d'opération.

C.2 – Les enjeux opérationnels d'une sécurité maîtrisée : SILRIA

SILRIA (Système d'information logistique de suivi de la ressource interarmées), expliqué par le lieutenant-colonel DUVAL, a pour objectif d'assurer la traçabilité des ressources logistiques en transit et de fournir un outil d'organisation des acheminements. Une fois la ressource initialisée par l'expéditeur, le logisticien exprime une demande d'acheminement-transport dirigée vers le CSOA. Le centre choisit le mode d'acheminement et réserve les vecteurs de transports qu'il priorise en fonction de la ressource et du théâtre d'opération. Une fois les ordres donnés, les ressources sont suivies car à chaque fois qu'elles passent un nœud logistique, un événement est créé ce qui assure la traçabilité. SILRIA permet d'offrir un outil de gestion des contenus mais aussi des contenants en en dressant l'inventaire (des conteneurs surtout). En bout de chaîne, l'unité réceptrice atteste la bonne livraison en quantité et en qualité en renvoyant les informations au système d'information. Concrètement,

l'utilisateur créé une unité à transporter (ce que peut être une ressource ou plusieurs) sur laquelle il colle une étiquette RFID disposant aussi d'un code barre. SILRIA permet de produire tous les documents de transit nécessaires à l'acheminement (douane, manifeste de transport de matière dangereuse). À partir du chargement et de l'expédition, le colis entre dans le système d'acheminement et est suivi tout au long de ses ruptures de charge éventuelles jusqu'à la réception. La technologie RFID utilisée est une identification par radiofréquence. SILRIA implique l'installation et la perception de nouveaux matériels : des terminaux spécifiques code barre (par souci d'interopérabilité avec les systèmes OTAN qui utilisent encore souvent le code barre), des portiques qui peuvent faire la lecture en groupe de colis et palettes, des terminaux qui peuvent lire les tags RFID passifs et actifs, des ordinateurs portables, des kits mobiles SILRIA (sur les théâtres), des imprimantes (pour les étiquettes), des points de lecture fixes RFID actif pour les zones de stockage des conteneurs.

Monsieur Patrick DELORME précise que derrière SILRIA se trouvent des modules qui permettent de traiter l'organisation du transport, le flux logistique et l'interface d'échange par exemple. De même, le module infocentre rend compte des opérations déroulées sur SILRIA. Le système s'intègre au programme SIA par des briques posées sur le STCIA au même titre que les briques de sécurité, de gestion ou de service technique. De fait, SILRIA bénéficie des programmes de sécurité du SIA. Une fois l'étude et l'analyse de sécurité faites, il existe des règles de bases pour assurer la sécurité des systèmes. Les terminaux spécifiques, les portes à quai, les antennes actives sont des points de vulnérabilités par exemple ; il faut mettre en place des mesures organisationnelles qui prennent en compte ces points de vulnérabilité. Il convient de noter, et cela est très important, qu'il n'y a pas de transmission Wifi sur SILRIA, décision prise afin de ne pas rentrer dans une difficulté de sécurisation des entrepôts du ministère de la défense.

Le capitaine PALACIO détaille trois grandes familles d'interfaces : les gestionnaires de ressource (SIMAT, SILCENT, ATAMS, etc.) qui fournissent à SILRIA le descriptif sur le colis à expédier, avec le gestionnaire de flotte (ARTEMIS) qui gère toutes les missions de transport métropolitain du CTTS au profit des armées et services et avec le gestionnaire financier (HERMES) qui contractualise les transports routiers vers des prestataires civils. Chaque interface produit des messages différents (colisage, acheminement, réception, demande de transport, confirmation/annulation de commande). Un module d'interfaçage

logistique (MIL), partie intégrante du STCIA, assure une médiation entre les systèmes partenaires et SILRIA, via un bus de service. Il est possible d'échanger par fichier, par web service ou par mail. En interne, un MES (deuxième bus d'échange) permet à partir du MIL de retransformer les messages pour qu'ils soient intégrés par SILRIA. Il existe plusieurs événements redoutés, tels que la perte d'un point de connexion entre SILRIA et les systèmes partenaires, une écoute des données en clair, un manque de contrôle de l'origine de l'information, une divulgation de données sensibles à des tiers ou encore un piégeage de la fonction transfert du fichier. Face à ces événements redoutés, des solutions sont mises en place : authentification pour accéder au MIL, PRI PCI avec un site de secours, contrôle des formats, règles d'attribution des messages par systèmes correspondants qui répondent à des règles de gestion précises, mécanisme de protection (certificats), journalisation des échanges.

Enfin, Monsieur Guy VENTURE expose les différents risques identifiés liés à l'usage de la RFID et les solutions envisagées. Il souligne tout d'abord la différence entre la RFID et le WIFI. Celui-ci permet d'accéder au réseau alors que la RFID capture uniquement une information. Dans le cadre de SILRIA, une étiquette transport (RFID passive) est produite pour être exploitée par un TS (PDA mobile) ou une porte à quai pour les gros volumes. Le côté actif est destiné aux conteneurs, il y a deux dispositifs possibles : le PDA mobile et le point de lecture fixe pour RFID active (PLFRA) pour capturer automatiquement l'information à l'entrée et en sortie de zone.

Quels sont les risques inhérents à un tel système ?

- Le clonage : il s'agit de reproduire à l'identique une étiquette ou un tag. Cette pratique est facile à réaliser car les normes respectées sont celles du marché et sont publiques. Pour contrer cette menace, nous pouvons associer le code SSCC au XTID (plaque d'immatriculation de la puce) ce qui nous alerte de la malversation.
- L'usurpation : dispositif électronique qui répond comme une étiquette mais sans reproduire le visuel. Le message produit n'est cependant pas parfait et peut être détecté par analyse du signal.
- Le déni de service : saturation ou brouillage d'un dispositif de lecture par émission d'un signal parasite. La parade consiste soit à chercher la source pour la neutraliser (*site survey radio*), soit à utiliser le code barre en alternative à la RFID.

- Le pistage : utilisation de la RFID pour suivre à distance un objet et donc un potentiel convoi militaire. Pour contrer, il est possible de mettre en sommeil le tag actif ou de le neutraliser sur le segment à risque.
- Le re-jeu : reproduction d'un échange radio après enregistrement, ceci est très difficile à mettre en place.
- Le relais : introduction d'un dispositif entre le tag et le lecteur qui permet d'éloigner le tag du lecteur en maintenant la connexion.
- La force brute : émission d'une série de codes aléatoires ou séquentiels pour pénétrer ou perturber un système pouvant aller jusqu'à provoquer un déni de service.
- La destruction : mise hors service d'un tag. L'étiquette peut être rééditée et le tag actif remplacé. Il faut surveiller les sites et faire en sorte qu'il n'y ait pas d'acteurs malveillants.
- Le transport illicite de données : certains tags ont une zone de mémoire capable de transporter de l'information à l'insu du transporteur. Cependant il n'y a pas de *user memory* sur les étiquettes SILRIA et quant au tag actif, il est blanchit à chaque nœud logistique ce qui réduit la portée de la menace.
- Le virus : théoriquement possible, mais très difficile compte tenue de la très faible mémoire disponible dans le tag RFID.

C.3 – Vue prospective des systèmes logistiques futurs

La vue prospective présentée par le colonel Jean-Louis VÉLUT se fixe comme horizon 2025-2030. La logistique est un monde complexe qui met en relation de nombreux acteurs. Lorsque l'on parle de soutien, on parle par essence d'un monde complexe. De plus, les armées françaises et l'armée de Terre en particulier doivent intervenir dans un milieu aéroterrestre souvent difficile, avec une occupation inégale du terrain du fait de la géographie, au contact de la population locale (amie ou hostile) et un déploiement de forces au sol souvent dispersé et disposant d'une faible autonomie logistique. Le soutien de ces forces terrestres nécessite donc des délais de mise en œuvre difficilement compressibles, depuis l'entrée de théâtre jusqu'aux unités de contact. Enfin, la logistique d'une opération reste évolutive et réactive en s'adaptant aux changements de rythme et d'intensité des engagements.

Le concept de soutien de l'armée de terre répond à plusieurs principes qui ont des conséquences sur les SIL :

- Unicité de la manœuvre : elle implique de faire converger et intégrer tous les métiers du soutien. Les SIL doivent donc être capables de faire la synthèse des données.
- Économie : les militaires ont le devoir d'économiser des ressources souvent limitées (ex : munitions guidées) et c'est notamment dans la précision des données fournies par les SIL que cette économie pourra être réalisée.
- Adaptabilité : lorsque qu'un déploiement logistique est effectif sur le terrain, il doit être adapté à la force. L'architecture des systèmes d'information, doit pouvoir faciliter cette adaptation.
- Continuité : le soutien des forces terrestres est un soutien permanent. Les liaisons de données et des serveurs doivent être sécurisées afin d'éviter les ruptures et pertes de données.
- Anticipation : le logisticien a besoin d'anticiper sa manœuvre. Il doit pour cela s'appuyer sur de fortes capacités de calcul, d'évaluation et de prévision.
- Réactivité : facilité d'utilisation du *software* (logiciel).
- Capacité à durer et à endurer : rusticité du *hardware* (matériel).
- Capacité à acheminer en tout temps en tout lieu : interopérabilité, notamment avec des alliés en coalition.

Les SIL sont actuellement en pleine évolution, ce qui permet d'optimiser les performances et de réduire les coûts financiers (alloués à l'entretien des SIL périmés). Leurs perspectives d'évolution sont nombreuses. En ce qui concerne la logistique des systèmes d'armes, la maintenance prédictive est une piste intéressante. Elle consiste à être capable de détecter grâce à des senseurs si certains systèmes ou sous-systèmes vont présenter des problèmes (usure, obsolescence etc.) à une échéance déterminée afin de prévoir le remplacement de ces composants. Dans un avenir proche, des objets connectés vont faire partie du quotidien du combattant, notamment dans le domaine de la santé (bracelet médical par exemple). La robotisation est une tendance croissante dans le domaine civil mais aussi militaire. Il est probable de voir arriver dans les dix à quinze années à venir les premiers convois semi-robotisés des hélicoptères dronisés, ou encore des opérations de manutention automatisées. Dans ce domaine, les Américains et les Israéliens sont en avance mais ces

technologies sont encore très coûteuses. Outre le rapport coût-efficacité, ces équipements posent des questions éthiques (quelle perception par les populations de convois robotisés par exemple ?). Prenant l'exemple du système d'information régimentaire (SIR) déployé dans l'armée de Terre, le colonel VÉLUT attire l'attention sur la nécessaire amélioration de l'interface homme-machine. Une interface trop compliquée nuit à l'efficacité d'emploi d'un système. Dans ce domaine, le monde civil propose des solutions très intéressantes.

L'armée de terre développe un plan de renouvellement de ses matériels : le programme SCORPION. Il tourne autour de l'arrivée du GRIFFON qui remplacera le VAB et du JAGUAR qui remplacera l'AMX 10RC. Au-delà de ces nouveaux véhicules SCORPION intègrera au travers de l'infovalorisation (l'optimisation de l'échange des données tactiques) tout un ensemble de systèmes d'arme. Dans ce cadre, un nouveau système d'information et de communication, le système d'information du combat Scorpion (SICS), sera au cœur de cette infovalorisation. Cette dernière concernera aussi la logistique. Par ailleurs, le soutien des unités SCORPION, très réactives et mobiles, impliquera sans doute la mise au point de nouveaux modes d'action logistiques.

Les risques cyber sont pris en compte dans les études en cours. Leurs origines peuvent être liées à des groupes organisées ou à des acteurs militaires hostiles. Même une approche *low cost* (comme l'extraction de données du Big Data) peut causer des dégâts considérables à une unité. Les attaques cyber peuvent impacter, par exemple, le monde de la santé et la confidentialité des données médicales, le soutien des moyens rares et cruciaux et les soutiens externalisés. Il importe donc de protéger les données tactiques et logistiques employées par nos forces afin de préserver leur sécurité, et si nécessaire, de permettre leur emploi dans le cadre d'enquêtes judiciaires. Finalement, les SIL sont les garants d'une logistique terrestre performante, si les vulnérabilités cyber sont bien prises en compte et des protections mises en place Dans cette perspective, l'adaptation et la formation des utilisateurs aux systèmes numériques de demain est cruciale.

D – Externalisation croissante et interconnexion à l'internet : atouts et dangers

D.1 – Interfaces militaires et industrielles supportées par les SIL : vulnérabilités et solutions

Dans le cadre du partenariat public-privé signé entre le ministère de la Défense et le groupement OPALE Défense (dont l'entreprise THALES fait partie). Monsieur Wulfran CHARNOZ présente l'organisation et les enjeux cybernétiques du système d'information conçu, déployé et géré par THALES sur le site de Balard (vu comme une extension de l'INTRADEF). Le système d'information est mis à disposition afin que le ministère de la Défense entrepose un certain nombre d'applications pour les exploiter. Le site géographique est protégé par des contrôles d'accès, de détection d'intrusion et de vidéosurveillance. Des salles blanches sont mises à disposition pour permettre au ministère d'installer les applications dont il a besoin. La partie CPCO, où la composante logistique est présente, est connectée au cœur réseau géré par l'industriel. Les flux supports de ces SIL passent par des SIC opérés par THALES. Leur disponibilité est gérée dans le cadre du partenariat. Pour ce qui concerne l'homologation de l'ensemble des SIC présents sur le site de Balard, de nombreux travaux ont été effectués, des analyses de risques, d'ingénierie et de validation, de sécurité. Disposer d'une homologation n'a de sens que si l'on maintient dans le temps un niveau de sécurité acceptable. Pour assurer une sécurité optimale, il y a donc nécessairement mise en place de MCS couplés à un certain nombre de mesures opérationnelles et techniques qui permettent de maîtriser les interfaces entre le système et les bases arrière des industriels. Le MCS consiste à pouvoir faire une analyse objective des vulnérabilités, mesurer les évolutions des niveaux de risques afin qu'ils restent acceptables et dans le cas où le risque dépasse le seuil acceptable pour l'homologation, il s'agit de mettre en place des patchs correctifs ou toutes autres mesures opérationnelles ou techniques nécessaires. Le processus de MCS comprend la phase conception et la phase exploitation. Quand on développe un système, il est nécessaire de la modéliser, ce qui permet d'automatiser un certain nombre d'actions au moment du déroulement du processus. Une fois que l'ensemble des alertes rentrent dans l'outil, un travail automatique analyse les caractéristiques de la faille pour calculer une première note CVSS

environnemental. Par exemple, si une faille est exploitable par internet mais que le système n'y est pas connecté, la faille aura beau avoir une note CVSS très élevée, au niveau environnemental, sa note CVSS restera assez basse. Cela permet de regrouper un certain nombre de vulnérabilités dans des niveaux CVSS moins critique pour le système et de les intégrer dans le cycle de MCO. Si les vulnérabilités restent fortes, une analyse plus fine s'effectue et peut amener à la conception d'un patch en urgence. Ceux-ci sont validés sur une plate-forme de référence chez THALES avant la production. Ces mesures visent à ne pas introduire de virus sur le domaine de confiance qu'est Balard et s'assurer que le produit installé sur le site est bien celui validé sur la plate-forme de référence. Toutes les données entrantes sont passées sur des stations blanches, toujours dans une volonté de lutte contre les virus. La disponibilité et l'intégrité des sites de Balard passent par la tenue de MCS et par l'assurance que les évolutions intègrent des mesures saines. La tendance actuelle, pour la partie MCO des équipements, intègre des stations de signature qui permettent de signer et de chiffrer les codes sources donnés au client. Cette mesure permet de s'assurer que ce qui est injecté dans un équipement est légitime.

D.2 – La Box@PME : une solution de sécurité déportée chez les sous-traitants

Ce projet, présenté par Monsieur Olivier MESNIL (Soprasteria) a pour but de sécuriser la *supply chain* de bout en bout. Actuellement, les grands groupes et l'État font appel à de nombreux sous-traitants particulièrement vulnérables. Dans l'aéronautique, 70 % de la valeur d'un avion est portée par des milliers de PME qui deviennent une multitude de potentiels points de faiblesse. Les PME sont beaucoup plus exposées que les grands groupes car ils ne disposent pas des mêmes moyens financiers ou humains. Partant de ce constat, le projet consiste à créer un réseau de PME pour une sécurité collaborative et mutualisée, de proposer un réseau de box liées à un cyber centre capable de réagir aux attaques, ce qui offre aux PME des moyens proches de ceux d'un grand groupe. Les PME vont percevoir des box qui collectent les éléments de sécurité grâce à des modules de veille, ce qui permet à chaque société de détecter plus facilement les attaques à son niveau et au cyber centre de détecter les attaques sur une plus grande échelle, au niveau de l'ensemble de l'écosystème, et ainsi

analyser l'objectif des attaques à une échelle plus large. Le centre procure de plus une aide en cas d'incident et un soutien aux PME.

Conclusions

Pour conclure ce séminaire, le colonel Jean-Charles NICOLAS, directeur des études et de la prospective de l'ETRS, adresse ses remerciements à tous les intervenants et les acteurs ayant participé à l'élaboration de ce colloque. Il s'agit de garder à l'esprit la nécessité d'avoir une approche globale pour apporter une réponse complète et de disposer de référentiels à jour permettant d'obtenir une cartographie fiable des systèmes déployés.

Si les SIL sont des SIOC, ils possèdent quelques spécificités qui leur sont propres. La logistique militaire est ainsi complexe et dépendante des opérations et de leurs tempos. Mais les SIL sont aussi des leviers d'efficacité indispensables à la manœuvre logistique sans laquelle la manœuvre tactique ne peut s'effectuer dans de bonnes conditions. Les systèmes, vulnérables, doivent être cybersécurisés sans pour autant nuire à l'interface d'utilisation et à la facilité de leur emploi. Les SIL se doivent d'être conviviaux sous peine de voir l'utilisateur trouver un biais détourné pour pouvoir remplir sa mission. Ils doivent être facilement administrables par la fonction SIC pour être efficaces et opérationnels. De par les interfaces nombreuses avec d'autres systèmes d'information – et notamment industriels – les failles sont potentiellement démultipliées. Il faut donc s'inscrire dans le temps long pour conserver le niveau de confiance nécessaire sur un système et pour cela pratiquer un maintien en conditions de sécurité continuel et en permanence évolution. L'avenir est riche en perspectives : objets connectés, maintenance prédictive, robotisation. Ces exemples ne sont pas encore des faits mais c'est clairement une dynamique qui va s'accroître dans les années proches. Il faut s'approprier d'emblée cette problématique. Les industriels montrent que des réalisations concrètes sont déjà fonctionnelles. Deux solutions techniques existantes ont été présentées au travers du projet Balard et de la solution de sécurisation des flux Box@PME. Elles sont source de protection et de sécurité dans les échanges d'information.

Ces éléments de confiance seront toujours indispensables pour que les utilisateurs disposent du niveau de confiance essentiel au bon déroulement des activités de leur profession, au service de la Nation.