Compte-rendu du séminaire du 7 avril 2015

« Cyberrésilience des systèmes d'armes à l'horizon 2020/2025 »

musée des Transmissions, Cesson Sévigné

dans le cadre des activités de la chaire Cyberdéfense et Cybersécurité

Saint-Cyr / Sogeti / Thales

Dans le prolongement des séminaires du 12 février 2013 et 12 mars 2014 ayant traité de la cyberconflictualité pour les Forces Terrestres et pour les Forces Armées, les écoles de Saint-Cyr Coëtquidan ont co-organisé le mardi 7 avril 2015 avec l'Ecole 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 le thème de la « cyberrésilience des systèmes d'armes à l'horizon 2020/2025 ».

Ouvert aux personnels de la Défense interarmées, il s'est voulu un lieu d'échange et de réflexion sur la question de la résilience qu'il convient d'aborder dès en amont de la conception de ces futurs systèmes des Forces Armées. Il a également été une opportunité de présenter la coopération effective entre ces trois acteurs du pôle d'excellence cyber de Bretagne, issue d'une volonté politique du ministre de la Défense Jean-Yves Le Drian de faire du Grand Ouest un acteur majeur de la souveraineté française dans le cyberespace, thématique dont l'actualité montre de jour en jour la pertinence.

Introduction au séminaire :

En introduisant le séminaire, le **général Yves-Tristan Boissan** a rappelé que le symposium des SIC 2015 avait déjà défloré le sujet dans une table ronde animée par le colonel Aymeric Bonnemaison le 13 février, en pointant la nécessité d'intégrer dès en amont de la conception de nos futurs systèmes d'armes leur sécurité face à des attaques Cyber, mais également de rendre possible lors d'une conduite d'opération la prise de mesures adéquates pour assurer le rétablissement d'un système d'armes, tout en s'assurant une capacité de continuité informatique.

Mais ces exigences, une fois exprimées, se doivent d'être approfondies afin de donner lieu à des actions concrètes, au risque d'adapter les approches classiques de programmation de nos futurs systèmes d'armes, ou de devoir adapter la conduite de nos opérations par la prise en compte de la menace Cyber.

L'ambition de cette journée était donc d'analyser les formes particulières de la résilience des forces armées à l'horizon 2025, horizon auquel la dimension cybernétique des opérations aura été pleinement intégrée dans l'architecture des futurs systèmes d'armes de la Marine, de l'Armée de l'Air ou de l'Armée de Terre.

Les principes généraux de la cyberrésilience :

La cyberrésilience est la capacité d'un système d'information à résister à une panne ou une cyberattaque et à revenir à son état initial après l'incident, ou bien comme la faculté d'un corps quelconque à retrouver ses propriétés initiales après une altération significative. La notion peut s'appliquer aussi bien à un système physique, qu'à un individu ou une organisation. Par définition, la résilience est une des propriétés fondamentales de l'institution militaire et l'entrée dans l'ère cybernétique ne fait que décliner sous une forme nouvelle une problématique aussi ancienne que les unités militaires.

Elle se traduit pour une organisation par sa capacité de continuer à fonctionner et de résister à des agressions internes comme externes, volontaires ou non. Le niveau de résilience se mesure à l'aune de critères tels que la structure de l'organisation mise en place, les ressources humaines consacrées au fonctionnement du système, la redondance et le durcissement des systèmes et des équipements, les procédures en place, des compétences acquises à travers une formation et un entrainement dédiés, la connaissance fine de l'état de fonctionnement du système et la capacité à diagnostiquer une défaillance potentielle.

Appliquée au cyberespace, la cyberrésilience implique donc de se préparer en amont, et de prendre en conduite les mesures adéquates pour assurer le rétablissement d'un système d'information et/ou de systèmes d'armes. En outre, l'aspect novateur de la résilience dans le monde cyber est qu'elle peut s'appliquer à des états où l'incertitude règne sur la sécurité des systèmes (virus déployés dont les effets ne sont pas maîtrisés), où l'intégrité du système n'est plus garantie, où l'activité du système peut être dégradée (données corrompues ou altérées) ou inopérante (communications inactives), où les risques de propagation des menaces sont possibles si les interconnexions entre systèmes restent ouvertes, l'ensemble pouvant nécessiter des bascules en des modes dégradés, ou l'isolement de certaines parties des S.I.

A l'ère de la cyberconflictualité, envisager la résilience des forces armées sous cet angle, mène à affirmer qu'elle se construit sur deux piliers indissociables.

- Le premier est un pilier technique : les systèmes d'armes doivent pouvoir faire face à une attaque cyber et, dans l'hypothèse où celle-ci ne peut être enrayée, retrouver leurs propriétés le plus rapidement et le plus complètement possible afin de permettre aux unités de poursuivre leur mission. Il s'agit donc de concevoir et de mettre en oeuvre des dispositifs de sécurité à la hauteur des agressions possibles, et des procédures de traitement des attaques et de reprise d'activité adaptées au contexte d'emploi particulier des forces armées.
- Le second pilier est un pilier humain et organisationnel : La résilience des systèmes d'armes ne peut être conçue isolément de la résilience de l'organisation elle-même. Il s'agit de comprendre comment une attaque cyber menée sur des systèmes d'armes essentiels pourrait mettre en péril l'organisation. La dimension cyber doit être pleinement intégrée dans la conduite des opérations de sorte que la crise cyber, si elle se produit, peut être gérée à sa juste mesure par le commandement, ce qui implique notamment de mettre en place les ressources humaines et les dispositifs organisationnels adaptés.

Plusieurs intervenants se sont efforcés durant une première session, de définir quels sont les principes généraux de la cyberrésilience dans la conception des systèmes d'armes :

Monsieur **Jean-Pierre Lebée** a ainsi rappelé le cycle de vie de la cyberrésilience : une prise en compte dans la phase de conception des systèmes par l'identification des risques et la protection des systèmes face à des attaques cyber, puis également durant la phase d'exploitation par la détection de ces menaces, la résolution des problèmes induits et la récupération post attaque.

L'identification des risques doit être analysée sous la double approche bottom-up (quels sont les risques sur les systèmes que je dois protéger) et top-down (quelles conséquences sur la mission), approche durcie au travers de scénarios joués (pentests entre autres) sur les systèmes une fois conçus.

La protection des systèmes hérite quant à elle du savoir-faire très ancien des technologies de l'information: redondance des systèmes, sauvegardes des données et leur restauration, sécurité (chiffrement, séparation des systèmes), règles drastiques de codage, fonctions Failsafe (comportement automatique du système évitant tout risque en cas de problème détecté) ; mais un savoir-faire qu'il convient de relire par rapport aux caractéristiques des vulnérabilités du cyberespace, en y intégrant de nouveaux réflexes de conception : fonctions de « traçage de traitres » dans les réseaux ad hoc, routeurs résilients ; ainsi que des règles s'appliquant aux organisations et personnels utilisateurs de ces systèmes : formation et sensibilisation des personnels, procédures de sécurité, règles d'hygiène informatique sévères, audits et contrôles.

En phase de déploiement opérationnel, des moyens de détection d'attaques cyber sont à mettre à disposition : des sondes techniques sur les réseaux et les systèmes effectuant des analyses de trafic et des remontées d'alarmes, des anti-virus intégrés, ainsi que des sondes métiers permettant d'identifier des attaques informatiques en détectant des comportements métiers anormaux. La France a d'ailleurs une volonté affirmée de souveraineté en matière de détection.

La résolution des problèmes, si elle n'est pas automatiquement intégrée dans les systèmes par des mécanismes temps réel en cas de très forte criticité, reste une question d'expertise qui nécessite une analyse humaine avant toute intervention ou déclenchement. Cette expertise implique en amont un entrainement des opérateurs, une gestion des configurations, et en opération des outils de supervision et d'aide à la décision, qui seront d'autant plus aisés à manipuler que des outils de visualisation graphique des problèmes les accompagneront.

La récupération est en final une phase de remise en exploitation nominale des systèmes.

L'ensemble de ces éléments se doit d'être pris en compte pour la résilience des systèmes d'armes du futur, mais qui plus est, dans toutes les phases du cycle de vie de ces systèmes, ainsi que dans leur environnement : transport, maintenance.

La détection et le traitement des cyberattaques sur des systèmes d'armes est donc un objectif majeur rappelé par le **lieutenant-colonel William Dupuy**. De basiques aux effets fugaces, jusqu'à complexes aux effets persistants mais nécessitant une mise en œuvre longue, les cyberattaques varient selon une gamme large et variée, dont un essai de modélisation a été réalisé par Lockheed Martin avec son modèle de Kill Chain qui liste 7 phases successives: Reconnaissance, Armement, Mise en place, Exploitation, Installation, Command & Control, Effets.

La caractéristique des systèmes d'armes, c'est que leur conception est élaborée dans des structures laissant très peu d'accès ou de prises aux cyberattaquants. Malgré la crainte de la félonie qui dans l'Histoire a permis la prise des forteresses les plus défendues, ces systèmes bénéficient d'une protection habituellement significative, non seulement par leur interconnexion aujourd'hui limitée, mais aussi car utilisant des technologies atypiques. Un attaquant a ainsi peu de moyens de les

étudier, ne disposant pas d'outils disponibles facilement, et ces systèmes étant peu interconnectés, sont donc difficiles à infecter.

Néanmoins, ces systèmes, peu étudiés par ceux qui pourraient aider à leur protection, ne peuvent être considérés comme protégés des cyberattaques. Astreints à des cycles de correction, validation et déploiement de solutions correctrices longs, ils sont non seulement vulnérables, mais également attaquables.

Or ils sont vitaux. Dès lors, il est absolument nécessaire de les surveiller en permanence, non pas par une surveillance statique, mais active. Il faut donc pouvoir estimer et s'adapter à un niveau de menace en ayant une analyse de risque proche de celle de l'attaquant, pour déterminer ses effets recherchés possibles. Le Cyber attaquant a en effet un but, des moyens, des modes opératoires, des enjeux opérationnels, mais l'ensemble est difficile à modéliser statistiquement. Il faut donc effectuer un pilotage constant, adaptatif, dont le but au final est de dissuader l'attaquant de s'en prendre à notre système, en tentant de penser comme lui, c'est-à-dire de compléter notre approche traditionnelle de la logique du maillon faible (un système est vu comme une somme de vulnérabilités potentielles) par une logique de l'effet maximal (une vulnérabilité n'est utile que dans l'avantage qu'elle fournit).

On pourra ici noter que certains systèmes opérationnels sont difficiles à mettre à jour car déployés sur le terrain. Portant, leur utilisation va permettre plus facilement de détecter les attaques pour lesquels ils seront potentiellement vulnérables, et ainsi améliorer à la fois la protection de ces systèmes et la résilience de l'organisation qui les utilise.

Selon le **lieutenant-colonel François-Régis Vigneau**, la cyberrésilience est avant tout une problématique opérationnelle avant d'être une problématique technique, ce que nous verrons plus en détail dans le paragraphe suivant. Elle implique à la fois des actions reflexes pour minimiser les impacts des attaques, et assurer une continuité du service, et nécessite une décision au niveau organisationnel avant de lancer le retour à la normale.

Les acteurs majeurs en sont les opérationnels métiers, avec l'appui des opérateurs et le soutien de la chaîne cyberprotection ainsi que des formateurs en phase de préparation.

En accompagnement de la préparation doit être d'abord réalisée une cartographie des systèmes et des données nécessaires à l'activité, les systèmes sous-jacents et les systèmes de soutien ou d'environnement. S'ensuit une analyse systémique, pour déterminer ses éléments les plus critiques, qui a la main sur les données, quelles indisponibilités sont supportables ou non, quel mode d'utilisation en dégradé est envisageable et pour quelle durée, ses points de fragilité unique (SPOF), et nos capacités d'action sur le système ; analyse qui permettra de définir le cœur critique du système et les niveaux d'impacts ou de dégradation possibles et acceptables, ou non.

Il devient alors possible d'étudier le plan de continuité et de reprise de l'activité et lister les processus de fonctionnement dans les différents modes ou états du système, ainsi que les limitations ou les impacts associés. Ce plan peut alors être soumis à validation, par une autorité et des organismes qui vont juger de sa faisabilité et de sa pertinence, puis testé régulièrement lors

d'exercices afin de valider son appui au maintien de la mission, entraîner les personnels et détecter les évolutions d'environnement, susceptibles de remettre en cause les solutions retenues.

La cyberrésilience s'apparente ainsi à un Processus Qualité continu, une boucle d'analyse qui évalue les solutions retenues et les problématiques que les menaces Cyber posent au niveau opérationnel lorsqu'elles sont détectées au cours de tests ou en action, et reprend l'analyse en fonction par une rétro boucle corrective. Le niveau de certitude n'étant jamais absolu, ce Processus Qualité doit être constant et vigilant. Pour exemple, certains Malware se réinstallent parfois toujours sur une machine, même si cette dernière est réinitialisée, par pénétration des systèmes de boot, indiquant qu'une action corrective n'est pas suffisante si elle n'est pas intégrée et contrôlée durablement dans ses effets.

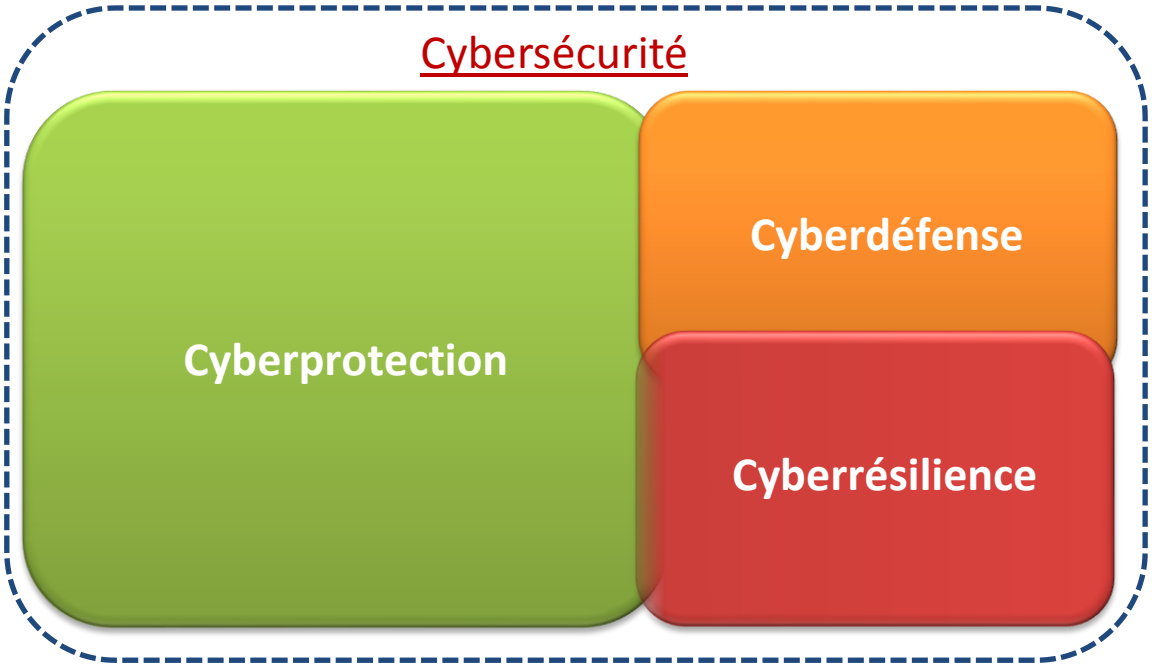
La cyberrésilience des systèmes d'armes : le cas Scorpion :

A la question de savoir quelle est la bonne démarche de sécurisation d'un système d'armes, **monsieur Philippe Leroy** de Thales a tout d'abord répondu en précisant les nouvelles contraintes spécifiques aux systèmes d'armes, notamment le fait que plusieurs composants de ces systèmes sont actuellement des COTS (Component on the Shelves) ou ont recours à des technologies civiles adaptées pour le monde militaire (Ethernet, Operating Systems, etc.). Les systèmes d'armes sont complexes et multiples, conçus de plus en plus souvent dans le cadre d'une coopération multinationale (OCCAR : A400, TIGRE…) et par conséquent devant tenir compte des soutiens industriels de chacun, des exigences de missions diverses et des contraintes d'emploi différentes. Le cycle des programmes d'armement reste significatif et doit intégrer les risques liés aux cycles d'obsolescence des sous-ensembles des systèmes (notamment des COTS). Car la technologie civile est maintenant prépondérante dans de nombreux domaines de l'évolution des systèmes d'information étroitement associés (ex : Cloud, mobilité des systèmes, sécurité applicative, etc.), avec des cycles de produits industriels plus rapides que ceux des programmes de la Défense.

En outre, la défense de nos systèmes se doit maintenant d'être active face aux menaces et à leurs évolutions, nécessitant un aspect technique de soutien proactif, dénommé Maintien en Condition de Sécurité (MCS) conçu en phase de définition du programme, mais également des volets plus opérationnels comme l'anticipation et renseignement, et la supervision active. Ainsi, comme composantes de la cybersécurité, si la cyberprotection est par nature statique, la cyberdéfense évolue résolument vers une posture active, et la cyberrésilience se doit d'être pro active, au croisement des deux premières composantes citées. L'anticipation des attaques (grâce au renseignement et à la veille proactive sur les vulnérabilités techniques) et l'adaptabilité en cas de problèmes (mécanismes et processus de résilience techniques ou opérationnels) sont à prévoir en amont, à l'issue des analyses de risques du programme. Par exemple, les procédures d'exploitation de sécurité, alimentées par les dossiers de sécurité et l'homologation initiale des SA, contribuent à cette résilience.

A cet effet, des études ont récemment eu lieu, notamment au travers de plusieurs PEA (ex : SARSYA : Sécurité des ARchitectures des SYstèmes d'Armes, qui ont conduit à la définition d'architectures résilientes concourant à la sécurité des systèmes d'armes, à travers la sécurisation des liaisons de données, la protection des informations sensibles embarquées par la définition de composants de sécurité locale et les moyens de gestion et de contrôle.

C'est donc sur l'ensemble du cycle de vie d'un système que doit se dérouler le processus de Maintien en Condition de Sécurité ayant pour objectif d'assurer sa disponibilité opérationnelle, maintenir son homologation dans la durée et assurer la cohérence de sa configuration face à des menaces par nature évolutives et de plus en plus ciblées.



Pour le système d'armes du futur pour l'Armée de Terre qu'est Scorpion, le **lieutenant-colonel Régis Demaie** a ensuite abordé la résilience dans le domaine cyber de ce programme en cours de développement, rappelant qu'il n'y pas de résilience sans protection et sans défense, et que le champ de la cybersécurité s'est largement étendu, passant par une formalisation plus précise du besoin de maintien en condition de sécurité pour tous nos systèmes.

Et s'il est d'usage aujourd'hui de comparer le dispositif général de la cybersécurité à une force qui doit soutenir un siège en s'abritant derrière des murailles (la cyberprotection), le lieutenant-colonel fait référence à Thucydide en affirmant que l'épaisseur des murailles n'est rien comparée à la volonté des hommes. C'est pourquoi la force dispose également d'une capacité d'action mobile, représentée par la cyberdéfense.

Un des points majeurs de la nouvelle instruction ministérielle 125-1516 qui régit les opérations d'armement, par rapport à l'ancienne, tient au volet maintien en condition opérationnelle (MCO), qui est devenu incontournable dans l'étude d'un programme. De même, le besoin de cybersécurité doit

être formalisé avec le besoin fonctionnel par l'écriture d'une fiche d'expression rationnelle d'objectifs de sécurité (FEROS), pour entrer dans la spécification technique que la DGA exprimera vers la main d'œuvre industrielle; par ailleurs, le maintien en condition de sécurité est l'élément majeur qui permet de s'assurer que l'on dispose d'un système dont le niveau de sécurité est pérenne, condition sine qua non d'une homologation.

Déclinée pour le programme Scorpion, c'est vers la cybersécurité du nouveau système d'information du combat Scorpion (le SICS) qu'il faut porter le premier effort de sécurisation. Ce système unique du chef de corps jusqu'au soldat regroupe à lui seul des capacités qui étaient autrefois disséminées dans le système d'information régimentaire et dans tous les systèmes d'information terminaux.

Quant aux deux nouveaux véhicules, le Jaguar et le Griffon, ils disposeront d'une architecture vétronique qui connectera entre elles toutes les fonctions de ces plateformes numérisées. De fait, toute vulnérabilité d'un composant peut avoir des conséquences sur l'ensemble de la plateforme, voire sur toute l'unité de combat, via les réseaux radio et le système d'information. Par ailleurs, la maintenance et la simulation auront leurs entrées dans ces plateformes, et l'ensemble sera en interface avec plus d'une trentaine d'autres systèmes numérisés. En conséquence, après avoir, dès sa définition, procédé à l'analyse de risques et exprimé son besoin, le programme Scorpion a formulé et transmis à la DGA une FEROS en vue d'assurer une cybersécurité au bon niveau pour ces équipements du futur.

Par ailleurs et de manière à assurer une résilience physique à la vulnérabilité des systèmes informatisés, des modes manuels mécaniques de secours sont prévus sur tous les systèmes, une panne informatique ne devant aucunement empêcher le véhicule d'assurer des fonctions essentielles à sa survie comme la mobilité ou l'agression.

Se basant sur le RETEX afghan d'une opération en 2009, opération au cours de laquelle deux virus ont infecté les réseaux de théâtre provoquant l'absence de remontées de situation tactique de référence, l'impossibilité de fournir les appuis nécessaires et la non transmission de certains ordres, monsieur **Philippe Mandle** a développé la notion de survivabilité d'un système, capacité d'un dispositif qui lui permet en mode opérationnel d'accomplir sa mission dans un contexte marqué par des agressions intentionnelles et tout en préservant la survie de ses constituants.

Dans l'exemple du GTIA Scorpion, la survivabilité consiste en l'évaluation de la gravité en terme d'impact opérationnel sur l'aptitude du GTIA à réaliser sa mission et en l'analyse de vulnérabilité des seuls constituants critiques du GTIA, mais non pas en la survivabilité individuelle des systèmes le constituant.

La démarche appliquée à Scorpion, nécessite l'identification des fonctions critiques (ex : localiser), l'identification des systèmes et des personnels critiques (personnels dont la perte entraîne une perte de capacité, équipements critiques, points faibles de l'organisation), et l'identification des menaces. L'étape suivante consiste en la maîtrise des risques par l'élaboration de parades qui peuvent être de parades systèmes (rajout de blindage, cloud tactique, …), organiques (redondance, …), utilisateurs (opérateurs), ou mixtes (passage en mode dégradé du système).

Prise en compte tôt dans la conception des systèmes, la survivabilité est une approche innovatrice, pluridisciplinaire, qui complète les approches systèmes classiques par une approche système de systèmes, au cœur des groupements tactique interarmes Scorpion de demain.

La cyberrésilience des systèmes d'armes : les systèmes aériens, maritimes et spatiaux :

L'avion de combat Rafale, qui a pour objectif de remplacer à terme 12 types d'avions différents de l'Armée de l'Air et de la Marine Nationale, est le système de Combat au cœur des missions Air/Air, Air/Sol, Air/Surface et Reconnaissance de la force aérienne française nous rappelle monsieur **Jean-Louis Guéneau** de Dassault aviation. Le RAFALE doit réaliser efficacement l'ensemble de ces missions et ceci jour et nuit, tous temps, sur tous les théâtres, parfois, souvent même, à grande distance dans des contextes complexes et en totale interopérabilité avec l'ensemble des forces nationales et alliées. Il doit garantir à ses utilisateurs une très grande efficacité sur tout le spectre des missions, grâce à la maitrise au bon niveau de la conscience de la situation tactique et de la survivabilité. La prise en compte du facteur humain est essentielle et impose des exigences de fonctionnement temps réel et non interruptible. Une consolidation de l'ensemble des informations critiques au sens de la sureté de fonctionnement contribue à la confiance de l'équipage en évitant les sources de désorientation « système ». Pilote/équipage centré, d'une grande flexibilité et capable de fonctionner en autonome, il effectue l'ensemble des missions défensives et offensives des avions de combat.

Le système embarqué du RAFALE concernent la relation avec l'équipage et toutes les fonctions de gestion du vol, de l'énergie, et de gestion de mission mettant en œuvre capteurs, communications, armements et effecteurs divers. Ce système est constitué d'un grand nombre de calculateurs propriétaires dialoguant au moyen de bus numériques dédiés. Le volume global des logiciels s'exprime en millions de lignes de code. Les caractéristiques principales de ce système sont une très forte Sureté de Fonctionnement démontrée, une réactivité temps réel, souvent non interruptible (on ne peut pas arrêter certaines fonctions sur un avion) et une interface équipage adaptée aux utilisateurs, qui permet le contrôle synthétique, mais complet des systèmes. La robustesse repose sur les exigences d'environnement ainsi que sur la segmentation et l'isolement des fonctions, la ségrégation technique tactique et sur la récente intégration du monde ouvert. La confidentialité est obtenue grâce à des dispositifs spécifiques (chargement et effacement des données sensibles, isolement des données confidentielles,…). Dans ce système où aucune panne simple ne doit interrompre la mission, la robustesse provient des redondances fonctionnelles et physiques, des surveillances et dissemblances. Enfin, le fonctionnement en modes dégradés, par exemple pour fournir le service en l'absence d'une partie des informations d'entrée a fait l'objet d'une attention particulière. Le système embarqué du Rafale est donc considéré comme très robuste aux défaillances d'origines diverses, ce qui contribue à sa résilience, avec des fonctions programmées par niveaux de criticité et de sureté de fonctionnement et dont le développement est réparti entre plusieurs industriels afin de garantir la confidentialité industrielle et de défense. Mais si ce système embarqué assure une redondance physique et logique, il est aussi l'élément d'un ensemble plus complexe qui est défini en cohérence avec les autres moyens des Forces Armées. A ce titre, il s'ouvre vers le monde extérieur au travers de l'interconnexion que le pilote peut emporter avec lui, comme des Smartphones ou des tablettes PC. Certaines composantes sont également sensibles car dépendantes

d'autres systèmes externes comme le GPS. Enfin les procédures otaniennes et l'application de standards, dont nous ne sommes pas propriétaires ont impliqué de séparer précisément le code souverain du code non souverain au sein de nos avions, pour parer à toute faiblesse sécuritaire.

L'ouverture des systèmes apporte de multiples défis qui sont évolutifs dans le temps. Ce sont cette ouverture des services ouverts, la coopération internationale, la standardisation des interfaces mais aussi l'utilisation de techniques duales, les soutiens externes et le risque d'une rupture technologique majeure qui apportent de nouvelles menaces pour nos futurs systèmes embarqués.

Pour y répondre, des mesures sont régulièrement prises, ou à prendre :

- de type organisationnel sur les personnels et les environnements (comme l'organisation et la répartition du travail, etc.), des mesures sur les matériels et logiciels utilisés (vérification, génération automatique, vérification d'intégrité, qualification), des mesures sur la maitrise de la cohérence du système complet (modélisation).
- de type protection des systèmes avec le choix d'une architecture de traitement de l'information soumise aux choix tactiques de l'équipage, l'implémentation de redondances physiques et logiques, chaudes ou froides, de contrôle (monitoring), de modes dégradés, de maitrise de changement des configurations logicielles, et d'une protection des données poussées (ex : gestion des clefs dans un réseau indépendant).

Ainsi, si nul système ne peut se permettre de rester figé, la résilience du RAFALE au risque Cyber repose actuellement sur une robustesse structurelle, avec des redondances fonctionnelles justifiées, matérielles et logicielles, et sur des modes compatibles avec l'absence de certaines informations. Néanmoins la vigilance est de mise, et implique une surveillance active des équipes Dassault dédiées à ces recherches.

Le **lieutenant-colonel Sébastien Vinçon** propose un élargissement de la réflexion pour rappeler que la résilience des systèmes d'arme ne doit pas être vue comme une finalité, mais comme un atout supplémentaire visant la résilience des activités.

L'Armée de l'Air a identifié 60 systèmes critiques, dont le Rafale n'est qu'un élément, certes central et incontournable. Pour assurer la cyberrésilience de ces systèmes, elle prône résolument une stratégie de dissuasion des attaques cyber, par les actions de ségrégation et de redondance des fonctions essentielles, en diversifiant les technologies, en renforçant l'agilité de reconfiguration de ses systèmes d'information car le temps de la réparation d'un système attaqué n'est pas celui de l'opération, et en renforçant l'organisation, les processus et les moyens opérationnels et de soutien de ses activités. Plusieurs plateformes de simulation sont nécessaires pour assurer la formation et la mise en place de cette stratégie, vue l'ampleur de celle-ci et le large spectre des systèmes critiques à couvrir.

Pour les bâtiments de surface de la Marine, le **capitaine de corvette Nicolas Malbec** a présenté les trois raisons justifiant le besoin en cyberrésilience des navires de combat : l'automatisation des systèmes, leur interconnexion et l'utilisation massive de systèmes d'aide à la navigation comme le

GPS, l'AIS ou les cartes électroniques. En ayant comme horizon 2020-2025, il a également indiqué ce que pourrait être un poste de combat cyber sur un navire du futur.

Les satellites militaires sont aujourd'hui des équipements incontournables assurant la coordination et le relais des transmissions sur une distance planétaire, notamment un lien avec la Métropole en opérations extérieures. Or un satellite ne se dépanne pas, ou peu avec quelques ajustements logiciels. Aussi la cyberrésilience doit être intégrée en amont de leur développement, nous indique le **commandant Xavier Houpe**.

Les satellites sont actuellement d'une grande complexité technique, afin d'assurer la résilience des communications en cas de problèmes ou de défaillances : de multiples redondances, des systèmes complémentaires, une autonomie de son ordinateur de bord. La résilience s'est aussi traduite au niveau organisationnel par des structures adaptées, et une gestion centrale redondée sur plusieurs sites, avec des réseaux cloisonnés. Les principes à adopter face à une attaque Cyber héritent donc de la même philosophie de résilience :

- Il ne doit pas exister de point de panne unique.
- Les passerelles entre chaine fonctionnelle nominale et redondante permettent une fiabilité globale. Plusieurs systèmes sont ainsi doublés, avec un nominal et un redondant. Certaines approches envisagent cependant à l'avenir, selon le capitaine de vaisseau Le Sellier de Chezelles, la mise en orbite de satellites plus bas coûts, avec une absence de redondance pour certains systèmes.
- Au sein du programme central, la fonction FDIR (Failure Detection, Isolation and Recovery) est composée de modules matériels (CRM), et de fonctions logicielles permettant de détecter toute panne logicielle ou d'un équipement qui pourrait induire une perte de la mission ou un dommage pour le satellite, d'isoler cette panne et de rétablir la fonction satellite et la mission grâce à une ou plusieurs actions à bord. Les séquences de reconfiguration peuvent être programmables par les équipes sol.
- Certains systèmes sont surdimensionnés (le nombre de cellules sur les panneaux solaires par exemple).
- Les systèmes de contrôle sont regroupés sur plusieurs emplacements géographiques.
- Interdiction de transmission de flux mettant en œuvre des protocoles standard.
- Simulation avant toute reconfiguration de la charge utile sur des plateformes à l'identique, plateformes où peuvent être rejouées tout problème.

Face à une telle conception de haute résilience, les attaques Cyber, si elles ne sont pas impossibles, ont néanmoins une faible probabilité de mettre en défaillance le satellite car les principes retenus dans le domaine satellitaire et concourant à la résilience garantissent dès à présent un haut niveau de sécurité. En outre, l'identification de l'attaque sera facilitée par le fait que les réseaux communicants avec le satellite sont homologués, donc sûrs sauf intrusion en interne. Pour parer à de telles éventualités, des exercices de dévolution sont régulièrement joués plusieurs fois par an. Enfin, en cas d'attaques de forte ampleur, l'autonomie du satellite doit lui permettre d'assurer le rétablissement minimal de ses fonctions.

La cyberrésilience humaine et organisationnelle :

L'organisation militaire se doit de faire face aux défis de la guerre cybernétique, et la réflexion à poser n'est pas uniquement une question de spécialistes des Systèmes d'Information. Au contraire, l'actualité nous montre les effets dévastateurs des attaques Cyber sur les Systèmes d'Information et leurs impacts sur notre société qui, s'ils ne se sont pas encore avérés mortels, montrent bien par transposition l'impact catastrophique que de telles attaques auraient sur nos systèmes d'armes. La résilience est donc un concept qui se doit d'être intégré dans la conduite des opérations et les composantes métiers qui y concourent, afin de préserver la conduite opérationnelle de la mission.

Monsieur **Gérard de Boisboissel** a ainsi tenté une modélisation de l'impact des attaques Cyber en séparant la cyberrésilience au niveau local (le système d'armes en lui-même) du niveau global (l'organisation des Forces Armées). Au niveau local, la cyberrésilience est une faculté de résistance du système à une attaque cyber et sa capacité de maintenir ou de rétablir son fonctionnement normal, dont dépend l'efficacité des organisations qui l'utilisent. Au niveau global, la résilience organisationnelle est la capacité à être robuste sous des conditions intenses de changement et de stress associé.

Au niveau local, des attaques cyber vont réduire le potentiel du système, ou sa qualité de service. Le système rentre alors en mode dégradé, dégradation tolérée si elle ne dépasse pas le seuil maximal acceptable, et qui sera rectifiée par des actions correctives.

A niveau global, une première caractéristique est qu'il apparait un décalage dans le temps entre l'attaque d'un système et sa perception par l'organisation, suivi d'un autre temps nécessaire pour son analyse. Une seconde est que la perturbation ressentie après une attaque n'est pas forcément identique à celle effective sur le système, elle peut être moins grave pour l'organisation (le système n'est pas un système critique, ou il existe un système redondant activable), ou plus grave. Prenons l'exemple d'un vol de données sur un système critique : ce système restera fonctionnel, et son efficacité sera toujours optimale, mais pour l'organisation, la menace que pose ce vol de données sur le système est très grave, et peut aller jusqu'à l'arrêt du système qui reste pour autant tout à fait efficace.

On ne peut donc affirmer clairement que la résilience globale d'une organisation est la somme des différents niveaux de résilience des chacun des systèmes locaux, ou même que la résilience globale du système est celle du plus faible des systèmes. Il est nécessaire de prendre en compte d'autres aspects pour son analyse au niveau organisationnel comme la prise en compte de certains facteurs sociologiques (le stress, la disponibilité humaine, la qualité de la formation des acteurs, ...), mais aussi managériaux (l'impact stratégique de l'attaque, ses risques de propagation, et la distorsion des effets qu'elle engendre ...). Une tentative de modélisation pourrait ainsi être :

- Mission = objectif + durée + moyens (qui sont les différents systèmes locaux)
- Risque mission = fonction (menaces, vulnérabilités)
- Perturbation système local = fonction (nature du système, dégradation du système, moment de l'attaque)
- Propagation = fonction (amplitude de l'attaque, durée, pénétrabilité des systèmes)

- Distorsion = fonction (effets de crise liés à l'attaque, criticité globale)
- Perception globale = fonction (Σ perturbation(s) des systèmes locaux + propagation + distorsion)
- Décision opérationnelle = fonction (perception globale, mission, risques mission, moyens)

La finalité de la décision prise par l'organisation est donc dépendante du contexte et de la criticité. Comme indiqué ci-dessus, elle prend en compte la mission, et lance les actions correctives qu'elle juge adaptée à la situation en fonction de son analyse de criticité et de risque liée à la crise induite par l'attaque.

La décision au niveau organisationnel peut ainsi aller à l'encontre d'une logique de niveau local, et déterminer une position allant dans le sens de l'accompagnement optimal de l'action militaire en fonction du moment, du degré de criticité des systèmes et de la mission. Ce peut être le rétablissement en mode nominal des systèmes dégradés, le choix de rester en mode dégradé, de basculer sur d'autre(s) système (s) redondants ou isolés, d'isoler les systèmes dégradés ou non, et éventuellement de faire évoluer la mission.

A partir de cette analyse, le **chef de bataillon Pierre-Arnaud Borrelly** propose de définir une séquence opérationnelle pour le Cyber dans l'action militaire au niveau de l'organisation :

- Renseigner – Alerter – Protéger – Entraver – Rétablir

Pour le renseignement et l'alerte, la problématique de l'anticipation tient en l'identification des menaces et à la supervision, qui passe par la qualité du renseignement et la qualité de l'alerte. Or, c'est l'incertitude d'un renseignement qui soumet l'organisme de conduite des opérations et de planification à une première situation de résilience, qui a été définie comme une plasticité de l'organisation pour continuer d'opérer et pour ajuster en permanence, ou au moins au rythme de sa boucle décisionnelle, son action.

Il est possible d'imaginer, par la logique de la notion d'effet utilisée en planification d'état-major, les différents résultats d'une attaque cyber pour sa résilience. Un effet est un changement d'état ou d'attitude, un résultat physique ou immatériel, une conséquence d'actions particulières à caractère militaire ou non militaire, visant une cible ou un objectif particulier. Au niveau opératif, il concernera les menaces globales du théâtre ou communes aux grands subordonnés, au niveau tactique il concernera les actions locales, les effets courts limités à la zone d'opération, et la traduction des effets opératifs.

L'effet résultant d'une attaque cyber peut effectivement être celui voulu par l'attaquant et se confondre avec l'effet ressenti par l'Etat-Major parce que l'organisation est faiblement résiliente et subie pleinement la volonté adverse. Il peut aussi y avoir une absence d'effet ressenti pour deux raisons : l'organisation est résiliente au point de la plus grande rigidité et ne mesure pas qu'elle fait l'objet d'une attaque et donc n'en tire aucune conséquence, ou l'organisation ne dispose pas des moyens de mesure et d'analyse lui permettant de prendre en compte la dimension d'une attaque ennemie à l'image d'un organisme vivant traversé par un rayonnement gamma. Enfin, le cas le plus courant, l'effet ressenti est différent de l'effet porté et il y a donc une distorsion de l'effet résultant

de la volonté ennemie. C'est dans le champ de cette distorsion durable que se trouve la résilience car elle nie à l'adversaire de faire peser pleinement sa volonté sur l'organisation.

La cyberrésilience serait ainsi le fruit de la combinaison d'une capacité de renseignement-surveillance (fonction anticipation et alerte), d'une capacité d'apprentissage (fonction analyse et formation) et d'une capacité à durer, tenir (fonction continuité de l'action).

Au niveau Etat-Major, le centre de gravité est une capacité (ou situation géographique) dont une force militaire ou toute autre entité (pays, alliance) tire sa liberté d'action, sa puissance ou sa volonté de combattre. Il est à la fois un objectif pour l'ennemi pour déstabiliser la force militaire visée, et pour l'organisation elle-même qui doit protéger au mieux ses systèmes vitaux. Le centre de gravité s'appuie sur des capacités essentielles (ses moyens principaux), qui nécessitent des exigences fondamentales (ressources nécessaires), mais soumis à ses propres vulnérabilités critiques (celles de ses éléments constituants). Pour être efficace, une attaque ou une défense recherchent à avoir un effet par l'atteinte dans le premier cas ou la protection dans le deuxième d'une vulnérabilité critique du centre de gravité.

Si ce centre de gravité permet d'identifier au sein d'une organisation le cœur de ce qui est vital au système, l'effort de résilience ne doit pas uniquement porter sur la protection de ses vulnérabilités qui se traduirait par une fragilité structurelle d'adaptation permanente sous contrainte hostile, mais pour être efficace se fonder sur l'adaptation aux besoins de l'action globale de ses capacités essentielles par une combinaison des logiques d'exploitation et d'exploration.

Sur le plan de la résilience du soldat et des unités face aux attaques Cyber, le **colonel Francis Chanson** entreprend une analyse de l'impact de la menace cyber sur le fantassin du champ de bataille, où traditionnellement l'ennemi est insaisissable mais réel. Or dans le cyberespace, l'ennemi devient immatériel et le combattant n'a pas conscience de l'origine de l'attaque. Une attaque cyber est donc vécue comme asymétrique, voire terroriste, et l'outil de combat perçu par conséquent comme inutile ôtant au soldat toute capacité d'action classique, ce qui est déstabilisant pour le combattant.

Face à ce mode d'action nouveau par l'ennemi, les facteurs déterminants sont le commandement au travers de ses capacités d'adaptation en conduite d'opération, et sur la formation. Tous les acteurs de la chaine cyber doivent en effet être formés, ce qui ne pose pas trop de souci pour les cadres officiers et sous-officiers, mais nécessite en revanche une réelle prise en compte pour les militaires du rang.

En tentant une étude comparative entre la résilience du cybercombattant et le combattant résilient, on constate pour ce dernier que les facteurs déterminants de sa résilience au combat sont l'absorption (la force du groupe aide à surpasser collectivement l'agression), l'adaptation et l'entraînement. Et si l'estime de soi pourrait apparaitre comme un facteur clef, il n'apparait pas évident que des Digital Native à l'aise devant des équipements technologiques soient plus résilients sur le champ de batailles que leurs camarades qui ne le sont pas. C'est encore une fois la force du commandement qui fera la différence dans l'épreuve au combat, et c'est donc un axe d'effort de formation supplémentaire pour les cadres militaires utilisant les systèmes d'armes de demain.

Selon le **colonel Jean-Charles Nicolas**, si aujourd'hui, la formation s'est densifiée fortement sur les volets cyberprotection et cyberdéfense, force est de constater que ce n'est pas le cas pour la cyberrésilience. En première analyse, il convient donc de mener une réflexion afin de lui consacrer une priorité équivalente.

De façon explicite, la cyberrésilience est décrite dans quelques documents permettant de comprendre et de mieux appréhender le sujet. Ainsi, la DIA 3.40, la cartographie des processus du MINDEF, des documents de la DGSIC décrivent la cyberrésilience. Si les aspects PCA/PRA et PCI/PRI sont bien explicités, il ressort particulièrement que la chaine de commandement des opérations d'une part et la chaine SIC d'autre part, sont les principaux acteurs de cette cyberrésilience en lien avec la chaine de commandement opérationnel de la cyberdéfense.

De ce constat, il ressort un différentiel notable entre une formation actuelle diffuse et clairsemée au regard d'un besoin estimé. Une mise en valeur des quelques actions de formation en cyberrésilience, le développement de formations spécifiques portant sur la robustesse des architectures ainsi qu' une meilleure prise en compte des capacités et services critiques seraient à même d'apporter une première réponse. De plus, il est essentiel de joindre à ce volet formation, un entrainement dédié à travers des séquences dans les exercices portant sur la gestion de crise et permettant de mettre en œuvre les compétences requises pour travailler en mode dégradé. En parallèle, un processus RETEX doit permettre de déterminer les marges de progrès et de faire évoluer nos concepts et actions de formations.

Au bilan, il s'agit bien d'établir une feuille de route avec les employeurs en matière de formation afin de prendre en compte la dimension cyberrésilience à son juste niveau.

Le **capitaine Antoine Roussel** a, pour terminer cette session, effectué un retour sur le parallèle que nous pourrions apporter entre la résilience des forces armées et l'évolution des technologies militaires au cours de l'Histoire. Il a, pour ce faire, présenté la genèse et l'évolution du système Gribeauval, premier système d'armes au sens contemporain du terme, adopté en 1764 suite au retour d'expérience de la guerre de Sept ans et fondé sur un compromis entre mobilité et puissance de feu. Pleinement opérationnel à partir des années 1770, ces matériels d'artillerie sont ensuite utilisés durant les campagnes de la Révolution et de l'Empire surclassant ceux des adversaires malgré une tentative de réforme aux dehors simplificateurs en 1803. Le système est d'ailleurs restauré dans sa pureté originelle en 1816 et ses principes reconduits à travers le « système Valée » jusqu'à l'adoption de nouveaux matériels en 1853. La longévité de ce système, la capacité des matériels à s'adapter à des contraintes opérationnelles différentes de celles qui avaient présidé à sa conception mettent en évidence le rôle des deux piliers de la résilience, technique et humain. Au plan technique, la collaboration avec les industriels (fondeurs) permet de rationnaliser et standardiser les matériels afin de faciliter les opérations de contrôle, de maintenance (interchangeabilité des ensembles et sous-ensemble à divers degrés) …, la doctrine d'emploi est guidée par les mêmes impératifs avec une spécialisation des matériels d'artillerie (campagne, place, siège et côte), des matériels dédiés (moyens de franchissement, de levage, forges de campagne, voitures d'artillerie), des officiers et des servants qui pour la première fois reçoivent une formation et un entraînement spécifiques favorisant

la manœuvre interarmes tout en créant une identité propre à l'artillerie. En fait l'adoption de ce système abouti également la création d'une arme de l'artillerie indépendante avec la mise en place d'une chaîne de commandement organique reposant sur des brigades et régiments permanents subordonnés au premier inspecteur de l'arme et d'une chaîne de commandement territoriale couplant centre de production, arsenaux, écoles et régiments. Enfin les modes de travail légués par Gribeauval (centralisation technique dans la conception et l'expérimentation de l'armement) sont consolidés par la création du Comité technique et du Dépôt central de l'artillerie en 1795, ancêtre de la Section technique de l'armée de Terre.

Conclusions :

Le but de cette journée de travail du mardi 7 avril 2015 était de présenter les différentes approches métier pour définir les principes de cyberrésilience, et de les compléter au regard des expériences de chacun afin de clarifier son périmètre, d'en déterminer les exigences, et de contribuer à sa prise en compte tout le long du cycle de vie d'un système d'armes.

Le **capitaine de vaisseau Le Sellier de Chezelles** a, pour conclure ce séminaire, défendu l'idée selon laquelle la cyberrésilience a aussi pour vocation à être intégrée dans la Cyberdéfense et la Cyberprotection. Il est désormais acquis qu'aucun système ne sera suffisamment robuste par conception pour résister dans le temps aux cyberattaques, et que nous ne pourrons anticiper une sécurité à 100% de nos systèmes face à des menaces évolutives. Il existe en outre toujours le risque de rupture technologique qui pourrait rendre nos systèmes de protection obsolescents.

Aussi, il apparait fondamental que cette notion de cyberrésilience soit prise en compte, tant sur le plan technique en l'intégrant dans la conception de nos systèmes d'armes, que dans l'organisation de nos Forces, à tout niveau décisionnel depuis le niveau des unités jusqu'au niveau de l'Etat-Major des Forces.

Cette cyberrésilience passe dans les faits par l'élaboration de mécanismes de résilience qui doivent être testés avant une éventuelle mise en œuvre par les organisations, ainsi que par la formation des personnels, à la fois des experts techniques qui opèrent les systèmes d'armes, mais aussi des décideurs à un échelon supérieur, apte à gérer les gestions de crise dans leur globalité. Mais cette réflexion doit s'ajuster au juste besoin, et inclure la notion de coût pour éviter toute redondance inutile dans les systèmes, et privilégier l'adaptabilité.

Il faut donc rester souples et vigilants, et s'appuyer sur des plateformes de simulation d'attaques adaptées à chaque métier.

CHAIRE DE CYBERDÉFENSE ET CYBERSECURITÉ

Gérard de Boisboissel,

Avril 2015