L'apport de la cyber dans la maîtrise des données opérationnelles

Jeudi 14 mars 2019 – CESSON SÉVIGNÉ Salle cinéma du COMSIC

Synthèse réalisée par Augustin de Gastines, chargé d'études au CREC Saint-Cyr

Présentation

Les données opérationnelles peuvent se définir comme les données qui vont pouvoir créer de l'information nécessaire et utile pour mener à bien les opérations militaires.

La numérisation de l'espace de bataille a inauguré une ère où la donnée est au centre de l'articulation des systèmes militaires leur permettant une meilleure efficacité et une meilleure réactivité.

Issues de sources plus nombreuses dont il faut assurer la fiabilité, tels que les capteurs déportés ou les objets intelligents, les données opérationnelles sont également enrichies de données complémentaires qui ne se limitent plus aux données relatives à l'état de nos matériels, à nos ressources humaines ou aux conditions d'environnement. Elles intègrent en effet des données issues de sondes actives analysant les connexions et les flux numériques en cours, ou issues de l'agrégation de données provenant de sources hétérogènes ou de corrélations entre évènements.

Ainsi, la numérisation s'accompagne d'une explosion du nombre de données servant aux opérations pour lesquelles il faut en assurer la maîtrise, c'est-à-dire garantir leur fiabilité et leur diffusion sécurisée. Les informations qui en sont issues doivent enfin être accessibles et lisibles par les décideurs opérationnels pour qu'elles puissent justement devenir utiles sur le plan opérationnel.

L'objet de cette journée d'études du 14 mars 2019 est d'aborder la nécessaire place de la cybersécurité dans la gestion des données opérationnelles, pour assurer une confiance dans leur présence au cœur des systèmes militaires.

Depuis 2013, dans le cadre des travaux de la chaire de cyberdéfense et cybersécurité Saint-Cyr Sogeti Thales, les écoles de Saint-Cyr Coëtquidan et son centre de recherche le CREC, le commandement des systèmes d'informations et de communication de l'armée de Terre (COMSIC) et la DGA Maîtrise de l'Information, co-organisent un séminaire portant sur les enjeux de la cybersécurité sur les questions de Défense. Dans le prolongement des 6 séminaires précédents, ce 7e nouveau séminaire porte sur le thème « L'apport de la cyber dans la maîtrise des données opérationnelles » et s'est tenu le jeudi 14 mars 2019 au COMSIC à Rennes.

Introduction

Général Olivier SERRA, général adjoint de formation - commandant de l'ETRS

Le Général Olivier Serra ouvre la journée de réflexion, rappelant qu'elle doit être un lieu d'échange constructif entre les armées et leurs partenaires sur des sujets d'intérêts opérationnels. Préoccupation majeure pour le monde civil, la maîtrise des données est un de ces sujets stratégiques pour les armées.

La multiplication des objets connectés participe de l'explosion des données. De la gestion des équipements à la santé du personnel, tous les champs opérationnels sont concernés. La maîtrise des données est donc vitale pour le commandement. À ce titre, la prise en compte du domaine cyber est une préoccupation majeure pour les armées.

Dans ce cadre, la surveillance des systèmes d'information doit être parfaitement maîtrisée afin de permettre l'efficacité opérationnelle. À cet effet, il a été mis en exergue trois maître-mots qui orienteront la réflexion et le partage de connaissances durant ce séminaire : connaître, analyser et décider.

- Connaître, c'est se connaître soi-même, c'est à dire être capable de surveiller et améliorer ses propres systèmes. Le rôle des SOC, qui permettent de prévenir les attaques sera abordé durant cette journée qui doit être une opportunité pour échanger sur leurs capacités.

- Analyser, dans un monde où les outils sont de plus en plus performants. Big data, machine learning, IA, hypervision, sont autant de sujets prépondérants dans un domaine numérique en pleine expansion. Or, détecter, identifier et mesurer des signaux d'attaque est un véritable défi, ces derniers étant de plus en plus faibles et discrets. Il s'agit donc d'analyser la manière dont les armées vont les exploiter afin d'optimiser le cycle décisionnel.

- Décider, notamment en contexte opérationnel où l'information est cruciale. Capteurs, objets connectés, SOC, nombreuses sont les sources de données opérationnelles. Il convient de transcrire ces données en information utile pour le commandement, quelques soient les évolutions des technologies dans le cyber espace. Il s'agit donc de réfléchir aux modalités de traitement des données, provenant de diverses sources, afin qu'elles soient exploitables par le chef opérationnel et permettent une prise de décision éclairée.

1. La sécurisation des données opérationnelles

L'exigence de la sécurité des données en opération et le rôle clef des SOC (Security Opération Center) : retour d'expérience.

Lieutenant Sébastien BREGENT, ingénieur, 807ème Cie.

Le Lieutenant Sébastien Brégent commence sa prise de parole par l'explication des divers systèmes d'information (SI) des forces: certains sont en effet classifiés, d'autres isolés, ou encore qui possèdent des logiciels différents. Le rôle d'un SOC est alors de défendre les SI. Il s'agit donc de surveiller, d'évaluer la menace et enfin d'appuyer les acteurs SIC pour éliminer le danger. Le but étant de conseiller au mieux le commandement. Pour cela le SOC doit être toujours actif, raison pour laquelle il y a deux cellules: une de supervision, puis l'autre d'analyse. Le chef du SOC fait une synthèse des informations données par ces deux cellules.
En opération, le SOC va être délocalisé pour être au plus proche du commandement par souci d'optimisation afin de permettre une meilleure communication. Cette délocalisation peut être, d'ailleurs, plus appréciée par les chefs d'opération, qui n'ont pas le sentiment de traiter avec des personnes. Sur le terrain, quatre sondes sont déployées afin de couvrir au maximum la zone d'action pour une plus grande efficacité du SOC.

Il convient de préciser que le SOC n'a pas une fonction de police, mais plutôt de sécurité des SI. En effet, il s'avère que la moitié des problèmes rencontrés est d'origine humaine, un tiers est dû à des vulnérabilités du système, un sixième est dû aux infections et seulement 5% en raison de véritables intrusions. En raison de la sensibilité des données opérationnelles, cela doit être sécurisé au maximum. Seulement tout ne pouvant l'être en raison de l'immense flux, il doit y a voir une sécurisation en priorité de certaines données.
Dernier point à noter, celui de la visibilité des SOC. En effet ils ne disposent pas d'une grande visibilité sur le terrain d'opération auprès du commandement opérationnel, ce qui entraîne des incompréhensions de la part des décideurs quant à leur rôle concret.

Présentation d'un SOC de la DIRISI (Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information)

Lieutenant-colonel Jean-Didier MATHIEU, chef de centre, DIRISI.

La Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information dispose de plusieurs SOC, en central à Maison Laffitte, le SOC DIRISI, et sur le territoire qu'on appelle des SOC Régionaux (SOC-R). Le SOC de la DIRISI a pour charge la supervision de la cybersécurité des SIC, c'est à dire, le volet technique des actions de cybersécurité comme l'explique le Lieutenant-colonel Jean-Didier Mathieu.
Un SOC supervise, mais en cas de menace des processus doivent être mis en œuvre pour une réaction ajustée. Cela se fait donc par une politique de journalisation et stratégie de supervision afin de détecter les menaces susceptibles d'avoir un impact sur les biens essentiels. Il y a ainsi un plan de supervision pour savoir comment repérer un élément redouté en créant divers scénarios de détection. Le véritable défi repose sur le difficile équilibre à trouver entre réduction de faux positifs, acceptation des vrais négatifs et faisabilité technique.
Il explique enfin pour finir les capacités matérielles, technologiques et humaines déployées pour faire face aux dangers.

De l'importance de la contextualisation dans un SOC.

Antonin HILY, directeur technique cyber sécurité, Sogeti.

Monsieur Hily nous présente le bilan sans appel des SOC réactifs: ils sont rapidement surchargés et assaillis de données. Cela représente 2 PetaOctets par mois. Le tiers des SOC est inefficace dans le monde en ce qui concerne la surveillance minimale pour laquelle ces derniers sont missionnés. Sur cent alertes relevées par jour, 30% sont de faux positifs. Ils reposent sur un modèle trop ancien qui se fait dépasser par les évolutions technologiques et le flux toujours croissant de données.

Il convient donc de dépasser cela en passant sur des SOC « pro-actifs » qui reposent sur un mode d'anticipation pour une meilleure mise en œuvre de la réaction, sur le déplacement du point pivot en ne mettant plus l'outillage comme centre de gravité du SOC, puis en donnant à la stratégie de gestion du renseignement sa place de cœur du dispositif. Les outils doivent être continuellement remis en cause et les informations stockées pour les utiliser au moment opportun. Il faut être en mesure de détecter les menaces avant qu'elles ne se déclenchent, passer donc d'un SOC réactif à un SOC pro-actif. L'enrichissement passe, entre autre choses, par l'intégration du renseignement : c'est la Threat Intelligence, l'art de manipuler le renseignement sur la menace et l'adversaire. Pour une plus grande efficacité M. Hily recommande de diversifier les « Threat Hunters », chasseurs de menace, en composant des équipes variées en termes de profils. Avec des analystes, des spécialistes de cybersécurité, mais également des psychologues, des statisticiens, sociologues… Ce qui nous conduit vers un plus grand champ de vue.
Sur des SOC pro-actifs le taux de faux positif chute à 0,5%, la clé est donc le renseignement et la manière dont on collecte les données.

2. La nécessaire prise en compte dynamique des évolutions technologiques

NATO FMN (Federated Mission Networking), une stratégie orientée « Data Centric Security ».

Laurent CAILLEUX, DGA-Maîtrise de l'information

Le concept de Federated Mission Networking de l'OTAN, présenté par Monsieur Cailleux, est une stratégie orientée « Data Centric Security » (DCS). Avec l'augmentation du volume des données, et donc une hausse des données de valeur, de nouvelles menaces apparaissent. Afin de faire face à ces nouveaux défis, la sécurité est centrée non plus seulement sur les réseaux mais sur les données elles-mêmes.
Le FMN créé en 2015, sous l'état-major ACT (Commandement Allié chargé de la Transformation), a pour but de fédérer les différentes capacités de la coalition pour faire coopérer les systèmes nationaux au sein de l'OTAN. La démarche FMN évite le partage limité des informations et les trop nombreuses passerelles de transmission. Malgré une communication qui demeure toujours compliquée avec certains délais, il y a une constante amélioration de la collaboration et de l'échange sécurisé d'information. Il convient de souligner une volonté d'améliorer la coopération civil/militaire (coopération CIMIC) dans ce domaine.
Dans le cadre des opérations de l'OTAN, il est nécessaire de protéger, contrôler et partager au mieux les données. Pour cela un nouveau modèle de confiance est requis, basé sur un label de confidentialité qui donnerait une architecture propre au système pour renforcer les structures. La vision DCS permet d'échanger des informations en opération extérieure par exemple, mais également avec des ONG en cas de catastrophes naturelles par exemple. Notons cependant que l'échange de données

(potentiellement sensibles) avec les ONG, pose la question de la prévention des fuites d'information. En définissant une politique de partage de l'information basée sur une stratégie commune de sécurité centrée sur les données, l'OTAN montre une volonté d'être toujours le plus efficace possible.
Quel avenir pour la démarche DCS? A ce jour l'action porte sur la poursuite des travaux pour une évolution permanente afin d'avoir une meilleure maîtrise des données opérationnelles.

Boucle courte spécification et développement: l'exemple de la détection des signaux faibles ou masqués en milieu aérien.

Erwan BOULAIN, direction innovation et prospective, La Ruche by Thales.

Monsieur Boulain débute son intervention par la présentation de La Ruche by Thalès en Bretagne. L'installation dans la région s'est décidée en raison du pôle d'activité qui combine les compétences cyber, la proximité avec l'INRIA et les relations avec l'Armée de l'Air.

Le concept de Cyber Air repose sur l'idée qu'il faille détecter les symptômes plutôt que les attaques. Ce dernier a pour objectif de détecter en temps réel tout comportement inhabituel, quand les méthodes actuelles mettent 200 jours en moyenne pour détecter une attaque nouvelle. Il ne convient pas de dire que l'un est meilleur que l'autre, au contraire, ces deux approches sont complémentaires. Mais une véritable prospective de la menace est vitale pour la détecter avant qu'elle n'attaque.
Ainsi en milieu aérien, on peut avoir recourt à l'Intelligence artificielle (IA) qui serait entrainée à détecter des présences potentiellement dangereuses avec des possibilités grandissantes en fonction de l'évolution des techniques. L'IA est développée pour analyser des trajectoires aussi bien de drones, d'avions, d'hélicoptères… L'IA recueille les données issues des radars et systèmes de détection pour déterminer des arbres de décision à partir de données d'apprentissage. Cette IA mesure alors le degré de « normalité » des données par rapport aux comportements appris. Le but recherché est de détecter des évènements d'une manière la plus précise possible en utilisant des règles souples pour contrer au mieux des anomalies non prévues. M. Boulain présente ensuite les résultats obtenus par les algorithmes sous forme de graphiques montrant les marges de succès, d'erreurs et d'amélioration (diaporama disponible sous intradef pour plus de détails). Les progrès sont ainsi notoires même si certaines erreurs persistent.

Comment faire face à l'explosion des données issues des sondes et autres moyens de recueil?

Ingénieur principal des études techniques de l'armement Thomas DEMONGEOT, chef prospective capacitaire au CALID (Centre d'Analyse de Lutte Informatique Défensive)

Le Centre d'Analyse de Lutte Informatique Défensive, dont fait partie M. Demongeot, collecte des données depuis les outils de sécurité, de prélèvements, de journaux d'évènements et de renseignements d'intérêt cyber. Pour faire face à l'explosion actuelle des données, une chaîne de supervision a été créée qui classifie les évènements selon leur importance. Ce sont des seuils qui permettent au service de ne pas être submergé par les alertes. En effet le CALID recherche dans de grands volumes de données.
Il y a un apport de l'IA dans ce domaine. Cette dernière traite les journaux et gère des requêtes pour détection d'anomalie. Le gain de temps et l'optimisation est considérable. Pour faire face à l'explosion des données, il convient d'améliorer constamment les algorithmes pour détecter des comportements malveillants qui sont de plus en plus discrets et donc compliqués à détecter. C'est notamment le rôle des spécialistes car l'IA collecte les données et les trie, mais il faut un accompagnement de l'analyse des résultats et définir les requêtes en amont, c'est à dire ce que l'on

recherche précisément. Avec l'amélioration des techniques, une IA capable d'accomplir ces tâches automatiquement d'une manière plus perfectionnée serait réalisable, même s'il ne faut pas négliger ni supprimer le contrôle humain sur ces fonctions. Les retours des analystes demeurent importants dans ce contrôle humain car il convient de faire apprendre des nouvelles compétences plutôt que de simplement les laisser aux mains d'une IA.

IA et cybersécurité

Thierry BERTHIER, maître de conférences, Université de Limoges, chercheur associé au CREC Saint-Cyr.

A de nombreuses reprises durant ce début de colloque, le terme d'IA et son apport a été prononcé, raison pour laquelle M. Berthier est intervenu pour nous expliquer l'apport que cela représente et des exemples très concrets d'utilisation d'une IA, ses vulnérabilités ainsi que ses voies d'amélioration. Il s'agit d'expliquer de quoi l'on parle lorsque l'IA est évoquée, son utilisation pour des actions défensives, puis offensives (False Data Injection), et la manière dont l'IA se révèle génératrice.
Quelques failles à prendre en compte:

- Question des virus intelligents, capables de se déclencher ou non suivant l'importance des données à atteindre: il s'agirait de faire en sorte qu'un virus puisse passer inaperçu à certains endroits pour mieux atteindre les systèmes plus sensibles et ce, d'une manière totalement autonome.
- L'IA génératrice: une intelligence capable de générer des empreintes digitales par exemple.

A partir d'une photo, l'IA est capable de générer un faux tableau de Van Gogh également. Il n'y pas d'atteinte à la sécurité des données opérationnelles mais l'on perçoit facilement qu'en développant plus ces aspects, cela représenterait un risque à venir conséquent pour la cyber sécurité si des personnes mal intentionnées en font usage.
Le diaporama complet est disponible sous intradef pour de plus grandes précisions.

3. La gestion de la cyber information

Quels indicateurs pour le tableau de bord pour les données opérationnelles?

Gérard GAUDIN, président R2GS.

Il existe 98 indicateurs opérationnels répertoriés à travers une liste dans laquelle sont notés tous les incidents, vulnérabilités et non-conformité propre à chaque indicateur, avec leurs statistiques donc.
Ces 98 indicateurs (génériques) sont applicables aux SOC militaires.
Ces indicateurs sont disponibles à travers le document suivant (disponible sous internet) : https://www.etsi.org/deliver/etsi_gs/ISI/001_099/00101/01.01.02_60/gs_isi00101v010102p.pdf.

Comment présenter les données (IHM, Cyberpicture) ?

Sylvain BAZINGUETTE, consultant cyber sécurité chez Sogeti.

Entreprises, fonds internationaux, places financières et ministères sont autant de lieux où la sécurité des données est vitale selon Monsieur Bazinguette. Les hackers et cyber-criminels s'attaquent de plus en plus à ces entités. Par conséquent, la veille des diverses formes de menaces est un service qui subit les mêmes lois que les autres services vendus par les entreprises: il en existe un business. Celui-ci propose un marketing reposant sur la peur et il convient de ne pas y céder en ce qui concerne la cybersécurité, sans pour autant négliger l'aspect vital qu'est la sécurité des informations. Ce

marketing propose parfois des promesses toujours plus grandes et généreuses, alors comment s'en sortir?
Les interventions précédentes ayant déjà évoqué les SOC, l'accent est cette fois mis sur les CSIRT (Computer Security Incident Response Team). Un CSIRT est à destination des entreprises et administrations, à la manière d'un SOC, sauf que les informations gérées sont disponibles pour tous. Il existe ainsi des offres de Threat Watch, l'exemple qui est fourni dans cette présentation concerne notamment SOGETI. Les offres de Threat Watch visent à déceler et anticiper les menaces d'attaques. En cinq étapes cela donne: Newsletter Cybersécurité, Veille des vulnérabilités, Threat Intelligence, Suivi typosquatting domaine, Exposition de données et d'assets clients (Etapes détaillées disponible dans le diaporama accessible sous intradef).

Management de l'information en temps de crise, comment intégrer les données cyber?

Capitaine François GERBE, chargé d'études au COMSIC/division études et prospective.

Le Capitaine François Gerbe explique à travers sa présentation de multiples définitions utiles pour comprendre le sens des termes expliqués. Comme le management des données, qui est l'activité organisant et entretenant les processus de collecte de données afin de soutenir le cycle de vie de l'information. Cela ne concerne que les organismes qui gèrent une grande quantité de données brutes. Il s'agit d'établir un ensemble de données de référence et d'optimiser la constitution des bases de données opérationnelles. La distinction est donc faite par le Capitaine Gerbe avec le management de l'information. En effet c'est une responsabilité de commandement dont l'ensemble des processus organisationnels et techniques garantissent la mise à disposition des informations pertinentes à la conduite des activités d'une organisation.

Le cycle de vie de l'information suit quatre phases principales:

1. Acquisition,
2. Exploitation,
3. Diffusion,
4. Archivage.

Se pose alors la question de la manière dont le chef interarmes utilise ces données cyber. Précisons que celui-ci ne les prendra en compte que lorsque les phases d'acquisition et d'exploitation auront été effectuées. Ces informations aident bien évidemment à la prise de décision du chef en mesurant les risques et en lui permettant de pouvoir disposer d'informations fiables.

Le décideur militaire au cœur des données et son action.

Chef de bataillon Clément GLEIYSE, 132e promotion, Ecole de guerre Terre.

La dernière intervention de ce colloque nous présente un aspect plus pratique de l'utilisation de la donnée, notamment du point de vue utilisateur, à savoir le militaire, en la personne du Chef de bataillon Clément Gleiyse. Les données opérationnelles sont essentielles à sécuriser car de l'information suit une décision qui créera un ordre d'action. Une bonne décision est celle qui fournit le meilleur rapport qualité-rapidité. Le chef agit de deux manières: il pense avec son expérience et avec la doctrine qui lui a été enseignée. Il en extrait deux types d'informations qui vont l'aider à prendre une décision au final.
Du point de vue militaire au cœur de l'action, l'attente est d'avoir une information qui soit fiable. Cette information doit être mobile afin de donner au chef une plus grande liberté d'action, tout en faisant en sorte que la sécurité des données ne soit pas reléguée au second plan.
Les nouveaux défis pour une donnée au service de la décision et de l'action sont alors:

- Le calibrage du pion de cyber protection de proximité
- La poursuite du recueil et de la mise en œuvre des idées jugées comme étant pertinentes.
- L’assurance d’une supervision du cyber espace au sein de l’Armée de Terre

Conclusion

Ingénieure générale Marie-Noëlle SCLAFER, directrice de DGA Maîtrise de l'information

Cette journée riche en enseignements et échanges nous apporte plusieurs éléments de conclusion que Madame Sclafer va mettre en lumière.
Disposer de données fiables, être en mesure de les protéger et les analyser est un aspect primordial mais pas pour autant nouveau. Cela est une exigence continue. Mais avec l'explosion du volume de données et de leurs valeurs, l'évolution porte sur le fait que les données tendent à être considérées désormais comme le cœur du système.

L'Intelligence Artificielle tient et tiendra sa place dans cette maîtrise. C'est une source d'enthousiasme avec ce qui pourrait être accompli, mais également d'incertitudes. Face à des logiciels en open source qui sont de plus en plus performants, le risque d'une utilisation malveillante est grand. Le danger est une rupture du système défensif. Faut-il alors se focaliser seulement sur l'évolution technologique? Il convient de trouver un équilibre entre cette évolution et celle des métiers. Le facteur humain doit rester un aspect majeur. Dans cette maîtrise, l'objectif est de pouvoir fournir une information concise et pertinente au décideur qui aura besoin de comprendre et utiliser cette dernière pour une meilleure capacité d'adaptation.

De même, ces évolutions technologiques imposent un nouveau tempo pour la réalisation de nos systèmes. Si on conçoit qu'un avion de combat ou un missile puisse demander des années de conception, de réalisation et de qualification, pour un système d'information il est nécessaire de raccourcir la boucle entre l'expression de besoin, la réalisation et la mise en service.
DGA, industriels et opérationnels doivent travailler encore plus étroitement pour un développement rapide, efficace et sûr. Les responsabilités vont être de plus en plus partagées dans les décisions et conceptions de systèmes. Il faut s'attendre à des bouleversements constants et se préparer à une adaptation continue des modes de coopération.

Dans cette coopération, l'attention doit être portée sur la captation des travaux académiques. Permettre une convergence entre industriels, chercheurs et la Défense est bénéfique pour tous, c'est l'ADN du Pôle d'Excellence Cyber et cette journée en est une illustration. Dans le lien civil/militaire le partage d'informations reste encore parfois difficile alors que c'est un intérêt commun. Pour remédier à cette situation, le ministère des Armées a le projet de mettre en place un lieu dédié pour permettre l'accès à de grands volumes de données au profit d'acteurs de confiance qui pourront ainsi partager leurs travaux de recherche, tester de nouvelles solutions ou de nouvelles briques technologiques.