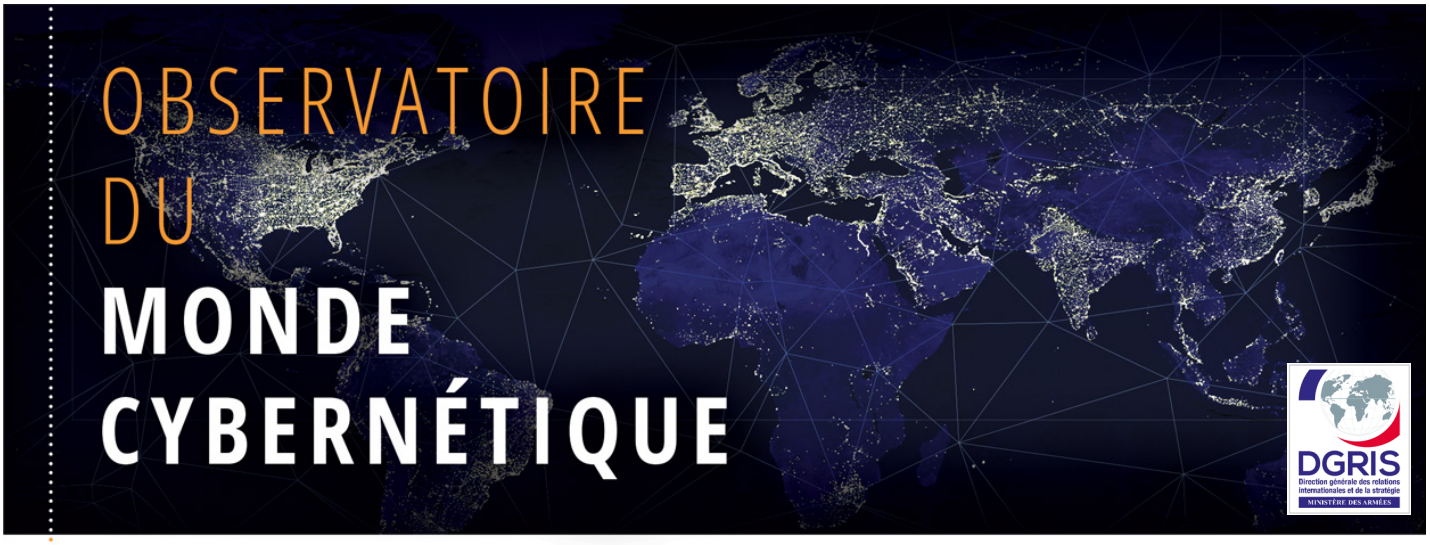


Lettre mensuelle – Décembre 2018 - disponible sur omc.ceis.eu

Edition Spéciale - Cyberdéfense et Entreprises

Défis et Technologies clés : anticipation, hypervision, résilience

CERCLE NATIONAL DES ARMEES 7 DÉCEMBRE 2018

Cette newsletter présente une synthèse des travaux du séminaire "Cyberdéfense & Entreprises : défis et technologies clés" qui a eu lieu le 7 décembre 2018.

Table des matières

ANALYSES

1. COMMENT RENFORCER LA RÉSILIENCE DES SYSTÈMES D'ARMES ?

Il est désormais communément admis qu'aucun système d'information ne peut être suffisamment robuste et protégé pour résister indéfiniment aux cyberattaques. De même qu'il reste impossible d'anticiper à 100% des menaces aujourd'hui très évolutives. Les systèmes d'armes n'échappent pas à ce constat dans un contexte de numérisation croissante des Armées, et notamment avec l'émergence de systèmes d'armes autonomes dotés d'une intelligence artificielle[1] ou hyperconnectés. Aux enjeux de cybersécurité s'ajoutent alors des enjeux de cyber-résilience de ces systèmes.

1.1. La cyber-résilience et son intérêt pour les systèmes d'armes

De manière générale, la résilience est la faculté pour une organisation de continuer à fonctionner face à des agressions internes comme externes, volontaires ou non, à leur résister, et à revenir à leur fonctionnement normal ensuite[2]. A la différence de la cybersécurité, qui caractérise la résistance d'un système d'information face à des cybermenaces, la cyber-résilience désigne quant à elle la capacité d'un système d'information à résister à une défaillance ou une attaque, et à revenir à son état initial après l'incident[3].

Le cyber-résilience couvre donc un périmètre plus large que la cybersécurité et appelle ainsi à concevoir la sécurité de façon systémique dans une approche qui implique à la fois les individus, les processus et les techniques. Appliquée aux systèmes d'armes, cette approche repose sur deux piliers indissociables, technique d'une part, et humain et organisationnel de l'autre :

- Un pilier technique : des mesures techniques de protection des SI, qui doivent pouvoir permettre aux systèmes d'armes de faire face à des cyberattaques, de continuer à fonctionner, même en mode dégradé, et de recouvrer rapidement toutes leurs facultés pour ne pas compromettre la mission pour laquelle ils étaient employés.

- Un pilier humain et organisationnel : les risques cyber pesant sur les systèmes d'armes peuvent mettre en péril à la fois le matériel et le personnel des armées et la conduite des opérations. Ceci nécessite du commandement et des composantes métiers de déployer des ressources humaines aux compétences dédiées et de mettre en place les dispositifs organisationnels adaptés pour intégrer la prise en compte de la dimension « cyber » à chaque étape du cycle de vie des systèmes d'armes.

---

[1] https://www.geostrategia.fr/vers-une-dissuasion-technologique-fondee-sur-les-systemes-darmes-autonomes/

[2] Voir sur ce point la Doctrine interarmées de Cyberdéfense DIA 3,40 : http://www.unor-reserves.fr/numero_en_cours%20A&D/Glossaire%20interarm%C3%A9es.pdf

[3] https://www.chaire-cyber.fr/IMG/pdf/synthese_colloque_7_avril.pdf

Ces deux piliers constituent les fondations des mesures qui doivent être mises en œuvre en amont du déploiement des systèmes d'armes, pendant leur déploiement, ainsi que durant et après la survenance d'un incident. Ces mesures doivent notamment permettre :

- L'identification des risques pesant sur les systèmes d'armes, et la protection des systèmes d'armes contre ces risques ;
- L'anticipation des attaques et l'adaptabilité des systèmes, à la fois aux particularités et besoins spécifiques de chaque mission mais aussi aux caractéristiques de l'environnement numérique et notamment aux conditions de connectivité pouvant les obliger à fonctionner en mode dégradé ;
- La connaissance des vulnérabilités des systèmes, et leur impact au plan opérationnel.

L'approche par la cyber-résilience permet ainsi de prendre en compte l'incertitude qui caractérise le milieu opérationnel, à la fois en termes sécuritaires (incertitudes sur les attaquants ou sur le type d'attaque) mais également en termes de fonctionnement des systèmes d'information (aléas météorologiques, mauvaise couverture réseau, chocs, etc. qui peuvent forcer à un fonctionnement en mode dégradé).

1.2. La mise en œuvre de la cyber-résilience des systèmes d'armes

Loin de n'être qu'une notion théorique, la cyber-résilience des systèmes d'armes s'incarne dans une série de mesures bien concrètes qui peuvent être mises en place en suivant plusieurs étapes.

La cyber-résilience nécessite d'adopter une approche globale des systèmes d'armes et passe par les étapes suivantes :

- **Garantir la robustesse des systèmes d'armes**

Tout d'abord, il convient de concevoir des systèmes d'armes robustes en durcissant les mesures de sécurité, notamment en :

- Empêchant les systèmes non sécurisés ou dégradés d'accéder ou de communiquer avec les autres systèmes ;
- Contrôlant l'accès aux terminaux utilisés dans le fonctionnement du système d'arme et leurs connexions (par des mesures d'authentification par exemple) ;
- Sécurisant les données utilisées dans le fonctionnement des systèmes d'armes et leurs circulations, notamment lorsqu'elles sont stockées dans le Cloud ;
- Sensibilisant les utilisateurs sur les enjeux de la sécurité de ces systèmes.

Le déploiement sur les systèmes d'armes de technologies de rupture, c'est-à-dire de technologies innovantes et peu voire pas encore adoptées, peut aider à diminuer ou éviter les risques liés aux défaillances et attaques contre les vulnérabilités déjà connues des technologies dominantes sur le marché, ou encore d'automatiser

les moyens de protection, de détection et d'alerte des systèmes d'armes. La détection peut jouer, en effet, un rôle important dans le déclenchement de mesures de cyber-résilience.

EXEMPLE DE SOLUTIONS PERMETTANT D'AMÉLIORIER LA ROBUSTESSE DES SYSTÈMES : ALGODONE ET YAGAAN

ALGODONE : la protection des puces électroniques[4]

Algodone a développé une technologie de protection des puces contre la contrefaçon baptisée SALT (*Silicon Activation Licensing technology*). Cette technologie permet d'activer ou de désactiver des fonctionnalités à l'aide d'une clé unique sécurisée (système de licences d'usage). En outre, elle permet de mesurer et de contrôler l'utilisation d'un composant dans le temps et dans l'espace. Ce type de solution rend possible la mise à jour d'un composant, de surveiller et de contrôler son utilisation et d'en protéger la propriété intellectuelle.

YAGAAN : l'audit de code source[5]

La solution de Yagaan permet de scanner le code source des logiciels pour en détecter les vulnérabilités en matière de cybersécurité. Cette solution combine l'analyse statique de code source avec l'intelligence artificielle, notamment le *machine learning*, afin d'adapter les alertes dans le contexte métier de l'application auditée. Cette approche permet ainsi d'éviter les risques de faux positifs.

- **Éprouver et tester les mesures techniques et organisationnelles de cyber-résilience**

Ensuite, il est primordial d'éprouver et de tester les mesures techniques et organisationnelles dans le cadre d'exercices de crise aussi réels et adaptés que possible mais aussi en envisageant les pires scénarios. Soulignons que les exercices de crise doivent impliquer l'ensemble des acteurs de la chaîne des systèmes d'armes (de la conception à l'utilisation).

- **Anticiper les risques et menaces cyber**

L'anticipation des risques et menaces par la mise en place notamment d'une veille au plan tant stratégique que tactique constitue également l'une des clés de la cyber-résilience des systèmes d'armes.

- **Responsabiliser l'ensemble des acteurs sur les risques cyber**

L'erreur classique consiste à n'impliquer que les responsables de la sécurité des systèmes d'information dans la mise en œuvre de la cyber résilience, et d'écarter les différents métiers impliqués dans le cycle de vie des

[4] https://www.algodone.com/

[5] https://www.yagaan.com/

systèmes d'armes. Cette approche qui témoigne d'un fonctionnement organisationnel « en silos » n'est pas adaptée à la cyber résilience qui appelle au contraire une approche globale.

Il devient en effet nécessaire de responsabiliser aux risques cyber les acteurs des différents métiers du cycle de vie des systèmes d'armes (conception, utilisation, MCO…), et de leur apprendre à travailler avec des systèmes dégradés et à savoir les remettre en état en cas d'incident. Cette responsabilisation peut se définir en amont par l'élaboration de procédures d'urgences qui précisent la conduite à tenir en cas de défaillance et les mesures et *process* pour rétablir le système et le remettre en état. Ces instructions doivent être diffusées auprès des personnes concernées pour que ces dernières puissent se former. Elle passe également par l'intégration du volet cyber dans l'entrainement quotidien des forces et par la montée en compétence par la formation de l'ensemble des acteurs concernés.

- **Améliorer continuellement la cyber-résilience**

Enfin, la cyber-résilience des systèmes d'armes doit être appréhendée comme un cycle d'amélioration continue. Son efficacité doit donc être régulièrement mesurée et adaptée. Cette approche permet d'assurer la résilience des systèmes d'armes dans le temps. Par ailleurs, notons qu'il est aujourd'hui impossible d'avoir une vision pleine et entière sur les risques cyber pesant sur les systèmes d'armes, et qu'il existera toujours des incertitudes sur leur sécurité lors de leur déploiement. Il convient donc de prioriser les éléments du systèmes d'armes à protéger en fonction de la mission comme de choisir le système de protection et la procédure de réponse incident les plus adaptés aux conditions de la mission.

2. L'INTELLIGENCE ARTIFICIELLE POUR AMELIORER NOS CAPACITES DE DETECTION ET D'ANTICIPATION

Les développements récents de l'intelligence artificielle (IA) rendent possible l'appréhension de volumes d'informations autrement inexploitables. En ce sens, les capacités de l'IA peuvent alors jouer un rôle dans l'amélioration de la détection et de l'anticipation des cybermenaces.

Aujourd'hui, l'IA suppose la combinaison des capacités suivantes :

- Une capacité de perception de l'environnement au moyen d'un apprentissage supervisé ou non ;
- Une capacité d'analyse et de résolution de problème ;
- Une capacité de proposition d'action, voire de décision autonome.

Concrètement, l'IA repose sur des algorithmes entrainés pour être capables de traiter rapidement des volumes d'informations massifs et d'en reconnaitre des éléments pertinents (un objet, une tendance, des corrélations, etc.).

Dans un contexte de numérisation croissante des Armées, les solutions basées sur l'IA peuvent offrir une véritable valeur ajoutée opérationnelle dans des domaines comme la logistique, la planification et la conduite des opérations ou encore le renseignement. En matière de cyberdéfense, se pose notamment la question de savoir si l'IA peut améliorer les capacités de détection et d'anticipation des Armées pour faire face à des cybermenaces toujours plus complexes.

2.1. Quelles utilisations de l'IA en matière de détection et d'anticipation ?

Des solutions d'IA permettent désormais de traiter de grands volumes de données et d'automatiser la détection en temps réel notamment :

- De vulnérabilités : tests d'intrusion automatisés, simulation d'attaques, détection de failles dans un logiciel ;
- De menaces internes ou externes : détection d'anomalies à partir d'une analyse comportementale, pour la lutte anti-APT, l'analyse de logs ou la lutte anti-fraude.

De nombreuses solutions reposant sur l'IA ont déjà fait leurs preuves dans le domaine de la détection, comme par exemple la solution basée sur l'analyse morphologique de Cyber-Detect(1). Ce type de solution permet aujourd'hui de détecter des comportements anormaux dans des systèmes d'information plutôt confinés comme les systèmes industriels. Pour les systèmes d'information classiques de type bureautique qui sont hyperconnectés, l'analyse comportementale des menaces reste en revanche encore difficile.

CYBER-DETECT : Analyse morphologique

Afin d'améliorer la détection des attaques informatiques encore inconnues, ciblées ou persistantes, CYBER-DETECT propose une solution d'analyse morphologique de codes binaires basée sur l'IA. Cette solution a la particularité d'identifier et de corréller les fonctionnalités d'un programme pour en prédire le comportement. Elle s'appuie pour ce faire sur des représentations multidimensionnelles du code analysé, et sur une base de comportements des malwares, là ou la plupart des autres solutions de ce type reposent elles sur des bases de signatures. La solution proposée par Cyber-Detect permet aussi de dépasser les mesures et outils déployés par les attaquants pour se protéger contre l'analyse de malwares, et permet donc de révéler le comportement de l'attaque.

En matière d'anticipation, les solutions basées sur l'IA offrent la possibilité d'identifier, très en amont, les signaux potentiellement annonciateurs d'une cybermenace. Elles sont donc notamment mises à profit dans le cadre d'activités de type Cyber Threat Intelligence pour la prévention des fuites de données, l'analyse et caractérisation des attaques passées, la surveillance des attaquants potentiels ou les tentatives d'attribution des attaques, c'est à dire d'identification des auteurs d'une attaque. Cependant, les solutions d'anticipation basées sur l'IA sont aujourd'hui moins matures que celles qui sont utilisées à des fins de détection. En effet,

l'utilisation de l'IA en matière d'anticipation est plus complexe à mettre en œuvre puisqu'il s'agit d'agréger des informations très hétérogènes. Néanmoins, il peut être intéressant d'utiliser l'IA pour améliorer la connaissance des vulnérabilités des systèmes d'information, et donc de repérer les failles de sécurité qui pourraient être exploitées par les attaquants.

De manière générale, renforcer les capacités de détection et d'anticipation contribue aussi à faciliter et rendre plus facile la prise de décision. Et ce d'autant que l'IA permet aussi le développement de la « cybersécurité cognitive », c'est à dire l'agrégation et le traitement de données non structurées (écrits des experts, réseaux sociaux, etc.) et structurées (logs par exemple) dans le but d'assister les équipes de sécurité dans la prise de décisions en temps réel.

2.2. 2. L'IA, porteuse d'un changement de paradigme en matière de cybersécurité.

L'utilisation de l'IA à des fins de détection et d'anticipation constitue un véritable changement de paradigme, avec le passage d'une « sécurité réactive » à une « sécurité proactive » qui s'adapte à l'évolution des menaces et aux malwares inconnus (2).

Ainsi, les solutions basées sur l'IA permettent de faire face aux limites des systèmes classiques de détection ou de protection en temps réel basés sur les signatures des malwares : nombre élevé de faux positifs, incapacité de s'adapter à l'évolution des menaces (APT notamment) ou encore lourdeur des bases de signatures affectant la performance des systèmes de détection.

Par ailleurs, l'IA apparait comme un moyen de pallier le risque de pénurie de compétence en cybersécurité. En effet, elle permet de décharger les équipes de sécurité de l'analyse manuelle fastidieuse des données telles que les logs. Ces dernières pourront alors se concentrer sur les évènements essentiels de sécurité.

En outre, l'IA sera également en capacité d'apporter une aide à la décision aux experts dans l'identification d'une attaque et dans la mise en œuvre d'un plan de remédiation.

Notons enfin que l'utilisation de l'IA pour la détection et l'anticipation des cybermenaces présente un enjeu organisationnel pour les futurs Centres Opérationnels de Sécurité (SOC). A l'avenir, les SOC devraient être de plus en plus automatisés, voire même interconnectés. Le SOC pourrait ainsi voir ses compétences de « détection et de réponse » muter vers des compétences de « prédiction et d'adaptation »(3). Aux États-Unis, l'IA rencontre déjà un véritable succès en matière de cyberdéfense. La DARPA américaine finance d'ailleurs plusieurs initiatives dans les domaines de la détection et de l'anticipation comme par exemple le programme CHESS (4), lancé début avril 2018, qui vise à combiner les valeurs ajoutées respectives de l'humain et de l'IA. En revanche, les solutions d'IA en cybersécurité ne sont encore qu'émergentes en Europe pour des raisons liées notamment à un manque de confiance dans les systèmes d'IA (5).

2.3. L'IA, entre promesse et méfiance ?

Si l'utilisation de l'IA en matière de cyberdéfense semble prometteuse, elle porte aussi certaines limites qui doivent être relevées :

Techniquement, l'IA présente un effet « boite noire », c'est-à-dire qu'elle ne permet pas aux utilisateurs de suivre et de comprendre les étapes de son raisonnement, ce qui peut avoir pour conséquence d'entamer la confiance qu'ils lui accordent. Le risque de faux positifs et les conséquences sur les décisions prises sur des bases biaisées qu'ils peuvent entraîner participent de cette défiance ;

L'IA ne saurait totalement remplacer l'intelligence humaine, qui reste nécessaire tant dans l'analyse des menaces que dans la prise de décisions, notamment lorsque ces dernières peuvent être lourdes de conséquences comme par exemple l'attribution d'une attaque.

La sécurité de l'IA risque d'être de plus en plus mise à l'épreuve à mesure que son utilisation se généralise, avec à la fois des attaques au niveau de l'apprentissage de l'IA que des possibilités de leurrer les systèmes basés sur l'IA.

2.4. Conseils et précautions de mise en œuvre

Afin de répondre aux limites précédemment évoquées et de mettre en place des solutions efficaces et fiables en matière de détection et d'anticipation des cybermenaces, plusieurs recommandations peuvent être formulées :

- Utiliser des algorithmes fiables, traçables et auditables (6) pour permettre à l'utilisateur de suivre et comprendre les étapes de raisonnement et les décisions prises par ou grâce à des solutions basées sur l'IA. Cette compréhension permettrait notamment de mieux appréhender les faux positifs, et donc d'améliorer le fonctionnement de ces outils ;
- S'assurer de la bonne qualité des données d'apprentissage qui doivent être représentatives des systèmes d'information à protéger ;
- S'assurer que le système d'IA procure une amélioration notable en matière de détection et d'anticipation en mesurant son gain de productivité, notamment le gain de temps (détection ou prise de décision plus rapide par exemple) ;
- Combiner l'IA et l'intelligence humaine au service d'une intelligence humaine augmentée : il s'agit de faire collaborer les spécialistes de l'IA et les spécialistes de la cybersécurité afin de mieux mesurer les résultats de l'IA. Cette approche « d'intelligence augmentée » existe déjà dans certaines solutions non spécialisées dans la cybersécurité comme MondoBrain par exemple (7).

MONDOBRAIN : L'intelligence Augmentée

Partant du constat que les techniques analytiques actuelles basées sur l'IA ont encore des difficultés à appréhender l'augmentation continue de données et qu'elles génèrent de nombreux faux positifs, MondoBrain a développé une solution qui fait converger :

- *La visualisation des données ;*
- *Les statistiques avancées ;*
- *L'intelligence artificielle ;*
- *L'intelligence collective (interactions entre les membres d'une équipe en cybersécurité par exemple).*

L'association humain-machine permet de prendre en compte l'historique des décisions prises par une organisation et d'appliquer des recommandations pour éviter les erreurs du passé et mieux anticiper les problèmes futurs. Cette solution analyse ainsi les données en fonction de la connaissance métier et peut donc s'adapter aux besoins de la cybersécurité pour améliorer la détection et l'anticipation des cybermenaces.

[1] http://www.cyber-detect.com/index-fr.html
[2] https://www.silicon.fr/dossiers/lintelligence-artificielle-au-secours-de-la-cybersecurite?inf_by=5b631d4e671db859418b4efa
[3] https://www.lesechos.fr/idees-debats/cercle/cercle-166576-le-soc-du-futur-sera-booste-par-lintelligence-artificielle-2066924.php
[4] https://www.darpa.mil/program/computers-and-humans-exploring-software-security
[5] https://www.lesechos.fr/24/01/2018/lesechos.fr/0301198805967_la-cybersecurite-veut-surfer-sur-l-intelligence-artificielle.htm
[6] https://www.alliancy.fr/le-numerique-en-pratique/symantec/lia-en-cybersecurite-trois-reflexes-simples-a-adopter-pour-choisir-plus-sereinement

3. L'HYPERVISION AU SERVICE DE LA CYBERDEFENSE

L'hypervision est la capacité de disposer d'une vision actualisée et globale du système d'information pour faciliter la détection et la réponse à incidents. L'hypervision est différente de la supervision en ce qu'elle procède à l'agrégation, au croisement et à la corrélation de nombreuses données techniques et métiers. En matière de cyberdéfense militaire, l'hypervision vise à donner aux opérationnels une vision large de l'état de fonctionnement de leurs systèmes. Une réflexion est en cours au sein des Armées pour intégrer de tels outils, qui ont déjà été testés. Toutefois, des investissements humains et financiers restent nécessaires pour un passage à l'échelle et une utilisation généralisée.

3.1. L'hypervision : une réponse à des systèmes de plus en plus complexes

L'émergence de l'hypervision, tant dans le secteur civil que militaire, répond à plusieurs besoins :

- Représenter simplement des réalités de plus en plus complexes et mouvantes (situational awareness) ;

- Croiser et corréler des typologies de données très différentes, comme les données topologiques sur le réseau, les données de situation, les données métiers, etc. : c'est ce croisement qui marque la différence avec une simple supervision ;
- Pouvoir utiliser le flux de données généré par l'hypervision à des scénarios de risque, afin de détecter au plus tôt tout incident ;
- Pouvoir partager différentes vues d'une même situation afin de faciliter les réponses aux incidents sur l'ensemble du périmètre hypervisé.

L'hypervision répond aux défis posés par la transformation numérique de l'ensemble des processus et activités et à la présence croissante de systèmes cyber-physiques. Elle répond également à la sophistication de la menace cyber, qui crée constamment de nouveaux besoins. Sur le plan technologique, de nouvelles solutions d'automatisation et de simulation commencent à apporter des réponses intéressantes grâce à l'Intelligence Artificielle.

3.2. Les composantes de l'hypervision

Contrairement à la supervision, l'hypervision fédère des domaines fonctionnels multiples. Une fois ce prérequis intégré, l'hypervision s'opère de la façon suivante :

- **Collecte** des données en continu grâce à des capteurs déployés sur l'ensemble des réseaux ;
- **Traitement et analyse** des données collectées : celles-ci sont structurées et corrélées ;
- **Visualisation** des données : cela passe nécessairement par leur modélisation (selon le contexte : modélisation réseau, modélisation de bâtiments, etc.) ;
- **Représentation** des informations : représentation de la réalité complexe grâce à un certain nombre de symboles définis au préalable entre les différents utilisateurs ;
- **Exploration et navigation** : ces fonctionnalités facilitent l'immersion de l'utilisateur dans la représentation et lui permettent de naviguer dans les différentes strates ;
- **Orchestration** : l'orchestration passe par l'automatisation d'un certain nombre de procédures, qui se déclenchent plus ou moins automatiquement selon les domaines ;

L'hypervision intègre également des fonctionnalités de **travail collaboratif et de simulation**, afin de pouvoir injecter des événements dans le dispositif et voir comment le système réagit par rapport à ces événements.

3.3. L'hypervision dans les Armées

Au sein du ministère des Armées, plusieurs entités assurent aujourd'hui les opérations de cyberdéfense des réseaux et systèmes d'information :

- Les SOC (*Security Operation Centers)* locaux, dont certains sont sous-traités, qui assurent la supervision d'une entité donnée ;

- Le CALID (Centre d'analyse de lutte informatique défensive), qui supervise l'ensemble des chaînes de détection du Ministère et génère ainsi une capacité d'hypervision ;
- Les groupes d'intervention cyber (GIC), mis en place de façon ad hoc pour la réponse à incidents ;
- Le Centre des opérations cyber (CO-CYBER), qui assure la conduite des opérations « cyber » en contextualisant la situation à l'aide d'informations fournies par d'autres acteurs (services de renseignement, alliés, forces armées sur le terrain, etc.) pour l'établissement et la mise à jour d'une « situation cyber de référence » (*cyberpicture*).

En 2017, un Commandement de cyberdéfense (COMCYBER) a été créé afin de répondre aux enjeux croissants de cybersécurité auxquels la France fait face. Le COMCYBER est placé sous l'autorité du Chef d'État-major des Armées. Interarmées, ce commandement rassemble dans une même chaîne fonctionnelle les forces de cyberdéfense des trois armées françaises. Le COMCYBER est composé d'un état-major (EM-CYBER) d'un centre opérationnel CYBER (CO-CYBER).

Le développement des capacités d'hypervision au sein des armées passera par une interactivité renforcée entre les niveaux tactique et stratégique, afin de créer des capacités de réponses coordonnées aux incidents, tout en étant économes en ressources rares (expertise et ressources réseau).

La mise en place de ces capacités devra se faire de manière progressive. L'établissement d'une doctrine pour encadrer et guider les pratiques sera également nécessaire pour mettre en œuvre l'hypervision. Cette doctrine devra être en mesure de s'adapter en continu aux évolutions des solutions technologiques en la matière.

3.4. Deux solutions d'hypervision : EGIDIUM et HYPERVISION TECHNOLOGY

Les sociétés EGIDIUM et HYPERVISION TECHNOLOGY proposent des solutions d'hypervision adaptées au besoin des Armées.

▶ ***EGIDIUM : Smart Shield et ISAP***

EGIDIUM est une PME créée en 2009 à partir d'une technologie issue du groupe AIRBUS. Elle édite Smart Shield1, une solution logicielle d'hypervision qui a vocation à améliorer la surveillance et la protection des emprises civiles ou militaires. Smart Shield permet de modéliser et de visualiser des emprises (maquettes 3D, plans 2D, cartographies, etc.) et à y insérer des informations issues des capteurs connectés (caméras, serrures connectées, détecteurs, etc.). Les systèmes d'information peuvent également être hypervisés avec Smart Shield Smart en les connectant à la plateforme, qui devient alors un hyperviseur physique et logique. Smart Shield est basé sur la plateforme logicielles ISAP (Integrated Security Automation Platform)2. ISAP connecte les capteurs, fusionne l'ensemble des données collectées et les structure avant de les restituer de manière contextuelle à l'interface Smart Shield. ISAP offre à l'"hyperviseur" la possibilité de percevoir la situation d'un espace donné, de savoir quelles sont les ressources déployées, quel est l'état du système et comme il est possible d'intervenir de la manière la plus efficace possible en cas d'incident. La plateforme est très ouverte : elle peut s'interfacer avec l'ensemble des capteurs et des systèmes existants. Smart Shield permet l'échange d'informations entre des structures qui n'ont ni la même organisation, ni le même langage : il est en effet capable d'analyser des vidéos, des images, mais également des sons, des logs, etc.

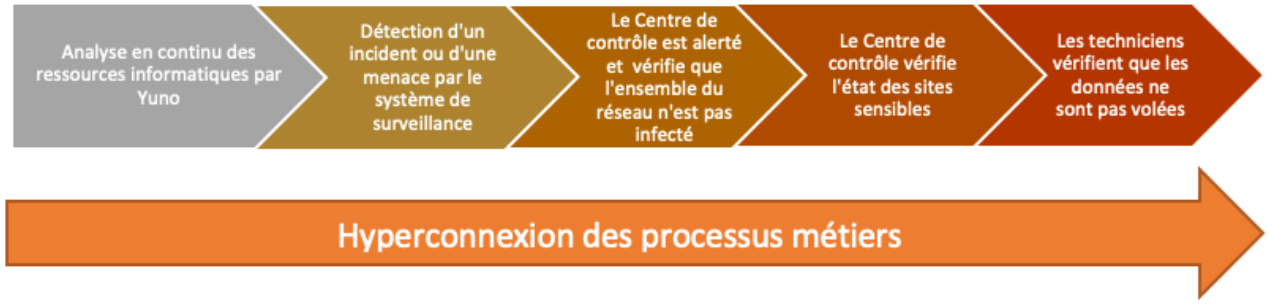
La solution intègre également une fonction d'aide à la décision, basée sur des outils tels que des alarmes, des typologies d'incidents ou encore des relectures de vidéos et du tracking de cibles. EGIDIUM fournit notamment sa solution Smart Shield à l'APOC (Airport Operations Center) d'Orly et au SIAE.

▶ *HYPERVISION TECHNOLOGY : Yuno*

HYPERVISION TECHNOLOGY édite la solution logicielle Yuno3, décrite par son fondateur, Xavier Laszcz, comme une "plateforme d'orchestration de réponse aux incidents et aux menaces". Yuno analyse en continu et en temps réel des données hétérogènes en provenance de sources diverses afin d'identifier les risques et les anticiper. HYPERVISION TECHNOLOGY est basée sur l'interconnexion de tous les processus métiers :

- *Ressources informatiques (datacenters, serveurs, bases de données, etc.) ;*
- *Supervision informatique et cyber : surveillance des ressources informatiques et alerte en cas d'incidents ;*
- *Centre de contrôle : analyse des alertes et déclenchement des actions curatives ;*
- *Techniciens : exécution des actions de résolution sur le terrain.*

Si un service entrant dans le périmètre de surveillance reçoit un email malveillant, Yuno va le détecter et isoler l'ordinateur. Le processus suivant se mettra alors en marche :



[1] https://www.egidium-technologies.com/fiche-solution-smartshield/
[2] https://www.egidium-technologies.com/isap/
[3] https://www.hypervision-technology.com

CALENDRIER

Les *Vauban Sessions*, 24 janvier 2019, Lille

L'impact de la Transformation Digitale sur les opérations militaire

Au cours de la dernière décennie, la transformation digitale et le cyber en particulier sont devenus des moyens pour améliorer l'efficacité des opérations militaires. Dans les guerres contemporaines, de la planification jusqu'à la conduite des opérations, le cyber est aujourd'hui une composante transverse des domaines terrestre, maritime, aérien et spatial. De nouveaux besoins pour l'entraînement nécessitant une approchante innovante en termes de technologies, de méthodes et d'usages, sont apparus, notamment pour les unités de réaction rapide de l'OTAN.

Les Vauban Sessions, organisées par le Corps de Réaction Rapide – France (CRR-Fr) avec le soutien de CEIS, se tiendront le **24 janvier 2019 à Lille.** Cette conférence réunira des représentants des forces armées alliées, de l'OTAN, des institutions européennes, des experts en cyberdéfense et de l'entraînement ainsi que des industriels et portera sur le thème de « **l'entrainement pour les opérations dans un environnement digital** ».

Parmi les intervenants :

- **Général (2S) Jean-Paul Paloméros,** ancien « Supreme Allied Commander Transformation » (SACT) de l'OTAN et conseiller sénior chez CEIS
- **Général Vincent Guionie**, Commandant des forces terrestres, Ministère des armées ;
- **Dr Gregory Edwards**, Directeur, Operations de Service, NCIA ;
- **Vice-Amiral Arnaud Coustillière**, Directeur Général CIS, Ministère des Armées ;
- **Général Wolfgang Renner**, Sous-Chef d'Etat-Major pour le Cyber, NATO Supreme Headquarters Allied Power Europe (SHAPE) ;
- **Général Jürgen Setzer**, Commandeur Adjoint pour le Cyber et le Domaine d'Information, Ministère de la Défense allemand ;
- **Jean-Paul Massart**, Chef, Formation et Entraînement, NCIA ;
- **Général Gérard Metz**, Sous-Chef d'Etat-Major, Eurocorps ;
- **Général Michiel van der Laan**, Commandeur 1 Corps (Allemagne/Pays Bas)

Les Vauban Sessions réuniront des représentants des forces armées alliées, de l'OTAN, des institutions européennes, des experts en cyberdéfense et de l'entraînement ainsi que des industriels, dans l'objectif de nourrir une discussion approfondie sur les éléments digitaux des opérations militaires modernes.

Pour toute demande d'information ou d'inscription merci de contacter frichardtixier@ceis.eu

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère des Armées

Direction Générale des Relations Internationales et de la Stratégie

60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS

Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15

Téléphone : 01 45 55 00 20

E-mail : omc@ceis-strat.com