« Les objets connectés et le monde militaire »

Mardi 21 mars 2017,

Salle cinéma du COMSIC - Cesson Sévigné

- **Introduction prononcée par madame l'Ingénieure générale Marie-Noëlle SCLAFER,** directrice de la DGA maîtrise de l'information**.**

Selon l'Ingénieure générale Marie-Noëlle SCLAFER, les objets connectés font partie intégrante de notre vie et en cela les perspectives industrielles qu'ils posent sont particulièrement intéressantes. La prolifération de ces éléments constitue un enjeu évalué à plusieurs milliards dans les années à venir. La technologie a rattrapé les systèmes militaires et certains usages sont déjà portés par la technologie (géolocalisation, suivi de l'état de santé, de la logistique, etc.).

Cependant, la sécurisation n'a pas été pensée au départ et les solutions sont mises en œuvre à postériori. Le niveau de la menace est très élevé et l'accompagnement des évolutions doit se poursuivre en prenant en compte la cybersécurité. Le risque est de bousculer les architectures existantes, notamment avec l'arrivée de la 5 G mais ces mutations sont inexorables et doivent donc être anticipées autant que faire se peut.

Elle insiste également sur le fait que ce séminaire suscite un grand intérêt car il permet des échanges fructueux qui feront évoluer les concepts et de trouver des équilibres entre poursuite des avancées technologiques et maintien de la sécurité nécessaire au bon déroulement des opérations militaires.

❖ 1. Introduction au Workshop

- **Etat de l'art des objets connectés : qu'est-ce qu'un tel objet, que fait-il et quelles possibilités offre-t-il ?**

Fulup AR FOLL, directeur de IOT.bzh (société lauréate du CWC 2016)

M. Fulup Ar Foll a entamé les exposés, en revenant sur la notion d'objet connecté et sur leurs possibilités.

Il en propose une définition très claire : « un objet qui interagit avec internet ou avec un élément lui-même en lien avec internet ». Leur nombre explose aujourd'hui dans nos sociétés. Les estimations parlent en effet de dizaines de milliards d'objets connectés à venir dans nos foyers.

Monsieur Ar Foll propose la classification suivante des objets connectés :

- leur taille et poids
- leur prix et le marché
- la consommation et la puissance
- l'autonomie et la recharge
- le système d'exploitation

Outre leur classification, leur introduction dans nos sociétés impose selon lui une analyse des risques, qui portent sur les quatre thématiques suivantes :

1. le risque financier
2. le risque pour la vie privée
3. le risque pour la santé des personnes
4. le risque politique et/ou étatique

Comme il l'explique, les objets connectés sont de différents types et chacun présente des caractéristiques différentes, qu'il s'agisse du système d'exploitation embarqué, des capacités offertes, de l'étendue des sécurités, des possibilités d'interaction et de développement (open source ou non) ou encore des facilités de mises à jour.

Ainsi l'on retrouve :

- Des « devices » ou capteurs aux capacités et à l'énergie plutôt limitées, dont la mise à jour est complexe. Leur système d'exploitation dédié offre peu de possibilités.
- Des « gateway » ou passerelles embarquant bien souvent Linux comme système d'exploitation, avec des possibilités de mises à jour plus larges mais restant difficilement accessibles. L'énergie et les capacités sont un peu plus étendues et permettent des calculs puissants. Ils souffrent principalement d'une absence de développeurs sur le marché.
- Le cloud qui offre une puissance illimitée, des possibilités de mises à jour si larges qu'elles demandent à être contrôlées. L'infrastructure du P*latform as a Service* (mise à disposition d'une plate-forme d'exécution) ainsi que la grande communauté de développeurs travaillant sur ce service permet d'envisager un large éventail d'évolutions.

Il est nécessaire de faire de justes choix dans les outils de développement afin de permettre une maîtrise des coûts, mais également de s'assurer un contexte sécurisé aussi bien dans le développement, que dans l'emploi et la mise à jour de ces outils. Notamment en isolant et compartimentant, ce qui est selon Monsieur Ar Foll la « seule option pour la cyber-résilience ».

Ce dernier termine son intervention en insistant sur la nécessité, dans les projets futurs pour nos forces armées, de faire émerger des besoins évidents et d'asseoir un cadre de développement avec des objectifs ciblés et des limites fixées. La tentation est grande de vouloir « tout faire », mais là est le risque d'arriver à un outil incomplet, non fonctionnel ou bien encore à un outil qui emporterait de trop nombreuses failles sécuritaires. Finalement, c'est le besoin d'une maintenance sur le long terme qui prime, celle-ci doit permettre la synchronisation et l'intégration continues sur toutes les plateformes et offrir des solutions de mise à jour « on-the-air », c'est-à-dire automatiques et à distance.

❖ 2. Besoins militaires et cas d'usage

Modérateur : Colonel Olivier KEMPF, officier transformation digitale de l'armée de Terre, EMAT

Cas d'usage des objets connectés pour les Armées.

Capitaine de vaisseaux Bertrand LESELLIER DE CHEZELLES, OCO en charge de la cyber des systèmes de communication, EMA/COCA.

Quand on parle des « objets connectés », aujourd'hui, on pense généralement aux objets de la vie quotidienne civile, mais lorsqu'on évoque les cas d'usage militaires il faut aller plus loin. Car ces derniers demandent une réflexion qui porte sur les 15 prochaines années.

Il faut savoir que les armées sont connectées depuis longtemps (exemple des systèmes de panneautage de l'amiral Nelson), car la « la connexion a toujours été indispensable pour les armées ». Ils permettent de nouveaux usages tels que les drones ou le combat collaboratif.

Cependant, les objets connectés présentent des contraintes pour les armées. Premièrement concernant les performances des réseaux de théâtre et le fait que ses objets soient développés pour des environnements permissifs (or la guerre se déroule souvent dans des lieux non permissifs). Aussi, les enjeux de sécurité posent la question de la maîtrise du spectre de fréquence (brouillage) et des risques cyber.

Enfin il y a des contraintes de tempo avec la formation et l'entrainement des combattants mais aussi le rapport entre le temps des programmes d'armement et celui des technologies. En effet un programme porte sur 10 à 15 ans et l'évolution technologique est trop rapide. Pour autant le combat de demain en sera pourvu avec un concept de bulle de théâtre dans laquelle les besoins de communication sont permanents, efficients, agiles et résilients dans une force interalliée.

Ainsi la question est de savoir : quel sera le combattant de demain ? Il devient une « usine à objet connectés permanente » ou plutôt une « usine à données » qui reçoit et envoie en permanence.

Pour conclure, le combat collaboratif est l'essence du combat futur et se fera avec une logique Iot. Le défi est de savoir si, du point de vue « programme d'armement », on dispose ou non des outils suffisants pour entrer dans l'ère de l'internet des objets.

Combat terrestre : quel emploi pour les objets connectés au contact ?

Capitaine Jean-Baptiste COLAS, officier de programme de l'armée de terre, conseiller innovation auprès de la DGA, STAT et DGA/UMESIO

Bien qu'il existe des usages intéressants, aujourd'hui les objets connectés sont prisonniers des systèmes :

- L'usage est lié à un dispositif précis.
- La connectivité est limitée.

- Les données sont prioritaires et cloisonnées.

Cependant, demain ils seront ouverts sur le champ de bataille :

- Adaptés au soldat par leur poids réduit, leur taille minimale et leur disponibilité élevée (autonomie et soutien).
- Collaboratifs car ils fonctionneront sur un modèle de données ouvert, posséderont des interfaces réseaux multiples et une capacité d'emploi basée sur l'opportunité.
- Simples et discrets car ils posséderont des interfaces de contrôle minimalistes et seront mis en œuvre par les plus bas échelons tactiques.

Ils permettront de placer le soldat au cœur du combat :

- Détecter la menace par le déploiement de capteurs morts dans la profondeur et périmétriques ainsi que le suivi objectif des capacités du combattant.
    - Audition déportée
    - Vision déportée
    - Bio censeurs
    - Cyber senseurs

- Comprendre son environnement par la présentation intelligible de la donnée permettant de discerner dans la complexité :
    - Cibler
    - Comparer
    - Partager

- Agir au combat par l'automatisation de ce qui peut l'être
    - Localisation
    - Désignation
    - Armes déportées
    - Nano usines, logistique distribuée.

Des enjeux critiques sont perceptibles :

- Des réseaux tactiques contraints.
- Les flux de données doivent être rendus exploitables.
- Les capacités « data mining et intelligence artificielle » sont limitées en opération.

A court terme, des solutions sont applicables :

- Des armes connectées grâce à une technologie simple et discrète permettant une accélération de la logistique (ex : dispositif permettant de compter le nombre de munitions tirées par une arme), apportant une plus-value directe au combat et une efficacité dans la gestion au quotidien.
- Des véhicules connectés permettant un contrôle à distance, une continuité embarqué-débarqué,

- Une maintenance prédictive et la possibilité de créer des pièces de maintenance grâce aux imprimantes 3 D.
- L'usage de drones terrestres ou aériens, permettant de s'affranchir des limites de portées radio.

Smart base d'Evreux : un exemple de développement d'objets connectés au sein de la pépinière numérique.

Lieutenant-colonel Bruno de SAN NICOLAS, commandant l'escadre aérienne de C 2 projetable (EAC2P), base aérienne 105 d'Evreux

Il présente deux exemples de développement d'objets connectés.

C'est au sein de cette pépinière regroupant startups et spécialistes des systèmes d'information que sont nées deux initiatives de travail.

a) La première est une technologie s'appuyant sur l'Ads-b, un système coopératif de surveillance du contrôle aérien, et baptisée ELIA : Équipements Légers d'Information via l'Ads-b.

L'Ads-b est un équivalent civil du radar de localisation militaire et présente l'avantage de permettre la multi latération, la localisation par émissions et par réponses aux interrogations de balises. Elle nécessite une précision de la mesure du temps d'arrivée des signaux, et une disposition géométrique adéquat du système formé par l'avion et les balises.

L'ELIA est né du constat simple que de nouveaux besoins se font ressentir pour nos forces, on distingue en particulier les besoins de :

- Récupérer des informations pertinentes en complément des moyens actuels, et que celles-ci soient indépendantes du réseau civil de l'internet ;
- Assurer l'optimisation pour nos forces de ces outils de détection, d'indentification et de communication. En particulier leur légèreté et leur faible coût ;
- Permettre la transmission de ces données vers les États-Majors et l'installation de ces outils aussi bien sur le territoire national, en zone hostile ou pourquoi pas dans un aéronef.

A l'aide de matériels issus du commerce, l'équipe projet est parvenue à créer l'un de ces équipements et peut aussi accéder à une interface issue d'un logiciel libre (open-source), et ce pour un montant approchant d'une centaine d'euros. Néanmoins ce système est très vulnérable et permet à n'importe qui, même sans moyens conséquents, d'accéder à la localisation en temps réel d'avions civils mais aussi militaires, ainsi qu'à un certain nombre d'informations (indicatifs, trajet etc.).

b) Un second projet - pour un montant similaire - appelé GeoCourtix, est un dispositif permettant la géolocalisation de personnel et la transmission de cette information par un canal sécurisé. Sa mise en œuvre doit aussi permettre de s'affranchir de la contrainte

économique que représente un vaste projet de renouvellement des matériels de nos armées.

A l'aide d'un microcontrôleur RPI[1] programmé pour recevoir des trames GPS et afficher les positions reçues sur une carte et d'un autre microcontrôleur Moteino capable d'envoyer ces données GPS, le personnel peut être localisé en temps réel. Une des perspectives possibles est l'ajout d'autres capteurs : capteur cardiaque, caméra etc. pour ainsi permettre l'envoi de ces données par le même canal.

Le lieutenant-colonel de SAN NICOLAS termine son intervention en expliquant que les technologies présentées ici sont à la portée de tous, qu'elles permettent de s'enrichir de la communauté open-source (avec également les besoins sécuritaires en terme de confidentialité que cela implique) et qu'elles permettent une grande hybridation (perspectives d'évolution) pour répondre, au mieux, aux aléas des théâtres de déploiement.

La captation de l'état physiologique du combattant

Médecin chef des services Stéphane BUFFAT, chercheur, IRBA / ACSO.

L'objet est la captation de l'Etat physiologique du combattant et pour cela, la prise en compte de la chaîne santé est importante (avant blessure, impact, triage, monitoring, soin, réhabilitation). Cependant cette réflexion s'inscrit dans un contexte particulier car il est difficile de définir ce qu'est la bonne santé.

Mais une vision complémentaire est possible avec la constitution d'une base de données sur le comportement humain. Car l'homme produit une grande variété de signaux externes (ondulation de la voix…) et internes (rythme cardiaque, ondulation vasculaire…).

Et la prise en compte de ses données nécessite de la rigueur et des conditions strictes proches du laboratoire. Concernant le cœur par exemple, recueillir des données cardiaques peut s'avérer inapproprié sur le court terme. De même la voix a une fréquence fondamentale identifiable mais celle-ci elle peut changer selon l'urgence, le stress.

Ainsi se pose les questions suivantes. Comment mesurer ? Et concernant le commandement, comment intégrer ces mesures dans une interface cerveau-machine ?

En conclusion les différentes démarches montrent l'importance d'avoir des données de qualité voire même des données enrichies avec annotations.

[1] Nano-ordinateur Raspberry Pi

- **Quel emploi des objets connectés dans les actions de maintien de l'ordre ?**

Général d'armée (2 S) Marc WATIN AUGOUARD, directeur du CREOGN

L'utilisation des objets connectés au sein de la Gendarmerie est un phénomène récent et le constat est que la progression de ceux-ci est fulgurante. Le déploiement du plan très haut débit (5 G) sur tout le territoire est une révolution annoncée. Cependant, il n'y aura pas de changements radicaux dans un proche avenir mais une évolution des pratiques professionnelles dans la Gendarmerie.

L'ouverture d'un chantier de réflexion sur l'apport des nouvelles technologies dans le maintien de l'ordre et la création d'une mission numérique, au printemps, devra permettre l'anticipation, essentielle à l'efficacité des forces de l'ordre. Savoir ce qui se passe sur le terrain, travailler avec le « big data », utilisation de la bulle informationnelle, pour faire face à la radicalisation de la violence est un enjeu stratégique dont les forces de sécurité doivent s'emparer.

Les objets connectés doivent permettre d'analyser le comportement des délinquants. Le maintien de l'ordre en zone rurale devient de plus en plus ardu, phénomène accentué par l'utilisation des réseaux sociaux. La situation d'échec de l'État à Notre Dame des landes en est un exemple.

Il est toutefois nécessaire de fixer un cadre juridique précis qui doit border l'utilisation des objets connectés.

❖ 3. L'architecture des systèmes d'information en support

Modérateur : Colonel Jean-Charles NICOLAS, conseiller cyber, COMSIC

- **De Felin à Scorpion : l'extension possible de l'architecture pour l'intégration des objets connectés.**

Sylvain METAIS, directeur technique ATOS / Bull

La société ATOS propose une offre en cyber sécurité qui couvre l'ensemble des besoins : la gouvernance et la supervision de la sécurité, les communications et les transactions sécurisées, le contrôle des identités et des accès numériques.

Le projet Auxylium de l'AdT a pour objectifs de:

- Fournir aux soldats un outil sécurisé de mobilité performant, rapide et réactif, avec une interface intuitive fonctionnant sur un terminal grand public, couvrant :
    - Les communications tactiques, s'appuyant sur un réseau LTE (civil ou militaire) ou un réseau MESH mis en place par les terminaux
    - L'enrichissement d'informations: géolocalisation, échange de données (cartes, positions, profils, demandes de soutien…)
    - Une gestion à l'échelon des groupes de combat
- Alléger le poids des équipements pour les soldats.

- Prendre en compte les usages inhérents aux technologies mobiles d'aujourd'hui et de demain en s'appuyant sur l'expertise des utilisateurs issue de la sphère privée (réseautage social, applications ergonomiques…)

- Un équipement utilisant les terminaux grand public pour réduire les coûts.

La sécurité des objets connectés passe un contrôle d'identité et des accès numériques permettant un accès sécurisé dans toutes les circonstances. Pour cela, le responsable de l'identité des accès doit gouverner, gérer et contrôler les identités et les autorisations des utilisateurs. Le responsable de l'authentification doit gérer une authentification stricte des objets.

C'est ainsi qu'a été approuvé par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) le premier smartphone sécurisé dès sa conception, le Hoox m2.

Le boitier TrustWay VPN de chiffrement (fournisseur Bull) permet de protéger l'ensemble de la chaine de sécurité par une intégration applicative (protection contre les intrusions, garantie de la confidentialité et de l'intégrité, fonctionnement sur tous les réseaux) et des performances élevées (chiffrement en temps réel jusqu'à 1Go/s).

Comment gérer des capteurs abandonnés connectés

Guillaume SIMENEL, directeur avant-vente SIGFOX

Le projet de SIGFOX est de « connecter le monde physique au monde digital » ce qui peut se décliner dans tous les secteurs.

SIGFOX est une entreprise mais aussi un protocole radio. Ce dernier s'inspire du monde sous-marin avec l'envoi de petits messages sur une longue distance.

Basé sur le réseau LPWAN il a l'avantage d'être : efficace en matière énergétique, global, économique et simple d'usage.

Economique car, il peut être abandonné (la perte étant minime : coût allant de 5 à 50 euros). Il se caractérise par le fait qu'en phase de veille il y a 0 message, 0 émission et ainsi 0 consommation d'énergie. De plus, avec l'amélioration des batteries et la prise en compte de la problématique de la collecte énergétique il est possible d'imaginer que la « durée de la batterie puisse être alignée sur la durée de l'objet ». Le réseau SIGFOX est global avec une présence dans 32 pays. Il se démarque par sa simplicité. En effet il se déploie facilement sans configuration ni appareillage.

Et surtout il est résilient, sa résistance au brouillage vient du principe même de son protocole qui implique une bande ultra étroite, une redondance géographique et un réseau collaboratif. De ces constats de nouvelles questions peuvent être abordées comme la question du cycle de vie, la problématique de géolocalisation des capteurs, de leur mise en quarantaine, leur abandon voire leur somnolence.

- **Emploi et architecture SIC des objets connectés, quelles incidences en matière de sécurité ?**

Colonel Patrick BIETRY, chef du bureau doctrine du COMSIC, ETRS division emploi COMSIC

Lieutenant-colonel Christophe PONS, chef du bureau cyber de la division emploi COMSIC, ETRS division emploi COMSIC

Les objets connectés dans le monde militaire ne sont pas une nouveauté, ce qui est nouveau c'est la rapidité du monde civil et le caractère dual de la technologie. Et ces objets vont se rencontrer sur le théâtre des opérations.

1/ Constat : Un paysage qui est transformé : Quelles seront les capacités de notre adversaire ? L'ennemi, l'adversaire qu'il soit asymétrique ou dissymétrique connaît une mutation. Il faut retenir qu'il a aujourd'hui accès à certaines technologies qui tendent à amoindrir sinon à annuler la supériorité que nous conférait notre propre maîtrise de ces technologies. Ainsi, il a accès aux technologies nivelantes connectées. Il est opportuniste, agile et avec un mode de commandement décentralisé. C'est alors pour nous la fin d'un certain confort opératif, il va nous falloir agir de façon décentralisée nous aussi.

2/ Nécessité de penser en système : Il faut se baser sur les 9 facteurs de supériorité opérationnelle mis en valeur par Action Terrestre Future. Car la performance du système de commandement doit assurer la direction optimisée des opérations par la prise en compte de quatre impératifs interdépendants, valables sur les théâtres extérieurs comme sur le territoire national : l'intelligence des situations, l'accélération des décisions, la plasticité des Organisations et la réduction des vulnérabilités. On observe qu'il y a plusieurs dimensions enchevêtrées (physique, humaine, temporelle), plus un défi cognitif. Mais il faut se méfier, car trop d'informations aboutit à un « chaos informationnel ».

3/ Volonté d'organiser le chaos : L'objectif est de fournir un double appui. Un Appui général : performance du commandement, agilité des PC, optimisation de la procédure de décision, maîtrise de l'information. Et un Appui direct : Accroissement de l'agilité tactique, augmentation du rendement de la force (éviter les dépenses inutiles du combattant). Pour les armées, l'intégration des objets connectés dans les systèmes d'information ou les systèmes d'armes (autonome de façon partielle ou totale) doit permettre la conquête de la supériorité informationnelle gage de la prise de l'ascendant sur nos adversaires. Cette intégration déplace le centre de gravité du besoin en sécurité vers le bas. Car il ne s'agit plus seulement de garantir la sécurité de l'information mais également celle de la donnée brute qui restera à valoriser et qui sera produite en masse. Compte tenu des contraintes les données collectées, transmises, stockées et traitées, devront être sécurisées au juste besoin et au juste temps.

Les enjeux de sécurité pour les forces sont primordiaux. Il s'agit d'adapter la cuirasse aux menaces du champ de bataille. Ce dernier répond aujourd'hui à un besoin de connectivité qui fait qu'il faut lier l'homme et l'objet. Car l'homme est au cœur de cette démarche, il est à la

fois le point d'accès au réseau et son extension en tant que producteur et consommateur de données.

Au-delà de ce besoin de connectivité, les forces ont aussi un besoin impérieux d'intégrité car toute donnée erronée peut faire échouer une opération. La supériorité informationnelle peut être réduite à néant ou inversée tout en laissant croire que tout est nominal. Garantir ce juste niveau de sécurité oblige à analyser de manière très fine le niveau de sécurité nécessaire à mettre en œuvre pour protéger aussi bien les systèmes que les informations et les données. Ces impératifs de sécurité et de connectivité peuvent être conjugués par un « arbitrage entre protection et production de données ».

Cela afin de conserver l'agilité d'action qui doit se traduire pour les unités par une modularité importante. Il s'agit donc bien de remettre la donnée produite, collectée, stockée et traitée dans son contexte d'emploi. Par conséquent, il faudra trouver un juste équilibre entre la préservation de l'agilité de la force et le niveau de sécurité requis.

Et surtout, il faudra préserver ces procédures même en mode dégradé car « l'avenir sera de passer du brouillard de la guerre au nuage de la guerre ».

❖ 4. Les problématiques de la cybersécurité des objets connectés militaires

Modérateur : David EUDELINE, Chef du département Ingénierie de la Sécurité des Systèmes (ISS), DGA

Typologies des vulnérabilités sur les objets connectés et analyse

Benoit MARTIN, adjoint technique SSI, DGA Maitrise de l'information

- Retour sur le séminaire César 2016, internet des objets : vous avez dit sécurité ? qui s'est déroulé du 21 au 23 novembre 2016 à Rennes. Les supports en ligne sont disponibles (restreint MINDEF) grâce au lien http://synoptic.intradef.gouv.fr/ressource-documentaire/cesar-2016

- Modèles de connexion dans le cyber espace
  Les objets connectés peuvent prendre des formes nouvelles dans le cyber espace : la réalité augmentée, la voiture connectée, la maison intelligente, les armes connectées.
  La prédominance de la sureté de fonctionnement ou de la cyber sécurité varie selon le type d'intégration dans les systèmes. La cyber sécurité est essentielle dans le prolongement de systèmes vers les capteurs intelligents (service à la personne, mobilité) ou dans les nouvelles composantes de systèmes complexes (inter action entre objets connectés autonomes). L'intégration répartie dans les systèmes complexes (domotique, automobile) nécessite une importance équivalente entre sureté de fonctionnement et cyber sécurité. La garantie de la

sureté de fonctionnement est essentielle dans l'intégration de flottille hiérarchisée dans les systèmes complexes.

- Vulnérabilités et menaces

  Les menaces sur le « hardware » sont parfois sous-estimées mais réelles :

  - Sensibilité des fonctions secondaires aux attaques (alimentation, horloges).
  - Signature du rayonnement.
  - Base matérielle corrompue (cheval de trois, contrefaçon électronique).
  - Absence de protection physique.
  - Mécanismes de protection limités (authentification faible, chiffrement faible.

Il est donc essentiel de se prémunir des menaces sur le logiciel par les actions suivantes :

- Capacité de mise à jour, y compris à distance.
- Journalisation adaptée pour les investigations numériques.
- Logiciels certifiés intègres et signés.
- Limiter les fonctions de l'objet connecté au strict besoin attendu.
- Garantir l'intégrité et la confidentialité des données.

- Démarches de cyber sécurisation

  Un certain nombre de mesure de cyber sécurisation existent :

  - Mise à jour et mise à jour de sécurité.
  - Chiffrement et authentification des communications.
  - Authentification des objets dans le réseau.
  - Protocoles standards et éprouvés.
  - Intégrité du code, confidentialité des données.
  - Primitives et protocoles cryptographiques.
  - Sécurité logicielle.
  - Sécurité matérielle.
  - Intégrité d'exécution.
  - Protection des données personnelles.
  - Journalisation des accès.
  - Intégrer l'objectif de sécurité tout au long du projet.

- Objets connectés dans le champ de bataille

  L'utilisation des objets connectés sur le champ de bataille sera liée à la prise en compte dès la conception des capteurs (borner les services au juste besoin), de l'architecture systèmes (intégration discrète ou en flottille, etc.) et des systèmes exploratoires (réseaux d'objets connectés autonomes). Il sera nécessaire de contrôler la dissémination liée à la miniaturisation et au faible coût et de maitriser les périmètres de responsabilité et d'administration.

La démarche de sécurité classique est applicable, mais il faut lever les freins liés au surcoût de la cyberprotection des objets connectés et en détection des cyberattaques et entreprendre une approche systémique.

- **Objets connectés et cyber sécurité : opportunité pour nos forces ? Quels sont les risques ?**

Michel BUZARE, chef de section zonale de contre ingérence cyber, direction du renseignement et de la sécurité de la Défense (DZRSD ouest)

Le but de la direction du renseignement et de la sécurité est de préserver les capacités opérationnelles de la Défense. La détection et l'identification des menaces font l'objet d'un effort important face aux nombreuses vulnérabilités avérées, décelés dans l'environnement des objets connectés. L'humain est souvent la source de failles et les objets connectés sont des moyens de renseignement. Les comportements déviants dans l'utilisation des montres connectées ou les smartphones (Pokemon) permettent souvent des intrusions et l'accès à des données personnelles.

La contre-ingérence doit permettre une meilleure protection des systèmes militaires.

❖ 5. Les solutions techniques de sécurité

Modérateur : Lieutenant-colonel Régis DEMAIE, Com DSI, ESCC

- **Entre contraintes d'autonomie et performance des objets connectés, quels niveaux de sécurité pour le chiffrement ?**

Damien CAUQUIL, responsable de la R&D sécurité et IoT, Digital Security

Les objets connectés ont plusieurs contraintes : notamment leur puissance de calcul limitée, leur capacité de stockage réduite, leur bande passante et enfin leur alimentation ou leur consommation. L'idéal étant d'avoir « une longue durée et un faible coût » avec une durée minimale voulue de 3 ans.

Cependant, les solutions du marché existent et permettent de gérer ses contraintes, avec notamment l'implémentation d'un mode veille, d'IRQ de réveil, de mémoires améliorées ou de modules d'alimentation optimisés.

Il reste une contrainte importante, celle du chiffrement notamment son coût monétaire et énergétique. Car le chiffrement « il faut le faire mais bien le faire ». Mal fait, il s'avère devenir une faiblesse comme nous le montre plusieurs échecs avec l'étude des cas des claviers Logitech et Microsoft.

De ces éléments se pose la question suivante. Quelles sont les sont les bonnes pratiques et solutions pour un chiffrement correct ?

On observe premièrement que le chiffrement dit « maison » n'est pas une bonne idée. Que l'AES est robuste et mais qu'il faut une bonne gestion des clefs. Car intégrer du chiffrement ne se fait pas sans une certaine rigueur. Il doit être doit être supervisé par des spécialistes. Des solutions fiables et optimisées existent (co-processeur crypto, Secure Elements). On peut aussi adopter une sécurité par *design* qui permet d'avoir une clef par objet et de combiner chiffrement et signature authentifiée. Mais cela a un inconvénient : c'est peu compatible et assez cher. Mais est-ce un coût négligeable face aux enjeux de confidentialité ?

- **Réseaux ad hoc, stockage distribué et pris en compte de la volatilité des objets connectés dans le monde militaire**

David BROMBERG, professeur des universités, IRISA / INRIA

L'enjeu primordial sera de connecter 50 milliards d'objets à l'horizon 2020, dans des systèmes complexes et hétérogènes, que ce soit dans le milieu civil ou militaire. Les évolutions liées à l'emploi du cloud pour traiter les données à distance seront la cible de toutes les attentions.

- **La technologie Block Chain et son application aux objets connectés militaires : théorie et cas pratiques**

Gilles CADIGNAN, président CEO, WOLEET

La question posée est de savoir si la technologie « Block Chain » est une solution de confiance adaptée pour les objets connectés militaires dans le partage d'informations, la mise à jour ou la logistique.

On peut distinguer des « Block Chain » privées ou publiques, présentant les caractéristiques suivantes :

Block Chain privée	Block Chain publique
Gouvernance de consortium	Absence d'autorité centrale
Infrastructure propre	Infrastructure publique distribuée
Modèle de sécurité différente, flexibilité	Sécurité, résilience, immutabilité
Nombre de participants limité	Nombre de participants illimité

Des projets notables sont d'ores et déjà exploités :

- L'IOT Chain of things : un consortium qui explore l'implication de la Block Chain pour la sécurité de l'IOT.
- La plateforme IOT d'IBM qui permet de connecter les appareils à la Block CHAIN privée Fabric (Hyperledger).

- FILAMENT : plateforme réseau sans fil sécurisée par Block Chain.

Des applications Block Chain orientées Défense sont envisageables dans les domaines de la logistique et du contrôle d'intégrité des données.

Les évolutions à venir devraient permettre, à partir de 2025, d'acquérir la confiance dans la donnée, en gardant une certaine sécurité.

IoT et solutions de cyber sécurité : la nécessité d'une approche globale

Patrice ROY, expert sécurité THALES Communication & Security

L'IoT peut être défini comme « **un réseau omniprésent qui permet la surveillance et le contrôle de l'environnement physique par la collecte, le traitement et l'analyse des données générées par des capteurs ou des objets intelligents** ». Il peut prendre différentes formes :

- Objet portable (*wearable*)
- Santé connectée
- Véhicule / Transport connecté
- Capteur/actionneur industriel (IIoT : Industrial Internet of Things)
- Domotique et contrôle d'accès
- Surveillance de l'environnement
- Gestion de l'énergie
- Gestion de l'eau
- Ville intelligente

On peut également trouver des exemples d'objets connectés spécifiques pour la Défense :

- La santé et la performance du soldat.
- Les drones et « Pocket drones ».
- Les lunettes de combat (enregistrement vidéo, vision nocturne améliorée, instruction de navigation, traduction en temps réel d'une langue locale, renseignement sur les sites ennemis).

De nouvelles exigences apparaissent :

- Un changement d'échelle : plusieurs milliers d'équipements à gérer.
- Une énorme quantité de données à stocker et à analyser.
- Un Traffic réseau, des technologies et des infrastructures hétérogènes.

Les vulnérabilités sont multiples de par les spécifications de sécurité faibles, voire inexistantes, l'architecture et le design qui permettent de nombreux vecteurs d'attaque, l'absence de mise à jour de sécurité, les guides de durcissement sur des équipements systèmes ne sont pas suffisamment respectés (ex : password faible ou par défaut, pas de contrôle d'accès réseaux, services inutiles non désactivés, etc.).

Une approche globale de la cyber sécurité de l'IoT doit être mise en œuvre et pour cela 4 fonctions essentielles doivent être sécurisées : l'acquisition de données, le transport, le stockage et l'exploitation. Pour cela, un mixe de solutions de sécurité doit être implémenté dans la protection, la détection, la dissuasion et l'organisation.

Conclusions :

- ✓ Des milliers d'objets connectés sur étagères sont et / ou seront vulnérables durant leur cycle de vie, et ils seront également présents dans le monde militaire…
- ✓ Une approche globale est nécessaire: Dans un environnement sensible, la sécurité de l'Internet des Objets doit être adressée depuis le design initial du système et de ses interfaces de communication jusqu'à son déploiement opérationnel et ce, tout au long de son cycle de vie (SDLC+MCS).
- ✓ Des challenges à venir :
    - Des mécanismes d'authentification robustes devront être mis en œuvre pour avoir une véritable chaine de confiance.
    - Des sondes de détection d'intrusion sur des protocoles de communication devront permettre d'identifier des tentatives de compromission d'objets / Gateway.
    - Un cadre réglementaire lié à la sécurité des objets connectés sera nécessaire pour obliger les industriels à implémenter des mécanismes de sécurité.

❖ 6. Conclusion du colloque

Général de Brigade Stéphane ADLOFF, commandant l'école des transmissions

Le général **Stéphane ADLOFF** a tout d'abord rappelé que nous entrons dans une nouvelle ère marquée par l'arrivée progressive d'objets connectés par milliards.

Pour lui, ce tournant implique un potentiel militaire qui n'est pas simple à cerner mais dont la plus-value opérationnelle est incontestable, à la condition d'un emploi mesuré et adapté de l'internet des objets. En effet, comme évoqué par plusieurs intervenants du colloque, un des principaux risques est celui de la surcharge cognitive du combattant. Ce dernier ayant déjà à s'assurer de l'exécution de ses ordres, de garder le contact avec la chaîne de commandement, il doit aussi être constamment en alerte pour garantir la sécurité de ses hommes et la sienne, sans même évoquer les divers aléas liés à l'action opérationnelle. L'apport nouveau de quantités de données à traiter peut aussi bien être une plus-value pour le soldat que perçue comme une charge incapacitante.

En réalité l'objet, devenant connecté, génère des données et avec elles, de la valeur. La problématique à laquelle il nous faut faire face aujourd'hui est celle de la valeur de la donnée. Le traitement de cette dernière sera essentiel et il s'agira de distinguer l'essentiel du superflu.

L’internet des objets permettant l’envoi systématique de données au bon interlocuteur, son apport à la numérisation de l’espace de bataille est incontestable.

Il est aussi à noter que la transmission de l’information d’un échelon de commandement au combattant lui-même nécessitera une grande protection. Cette sécurité de l’information doit être garantie car c’est la sécurité des femmes et des hommes de nos déploiements opérationnels et, plus largement, la réussite de la mission qui sont en jeu. L’action primant sur les délais de procédure, ce facteur n’est pas à négliger, autrement cette technologie ne pourra, et ne sera pas utilisée.

Finalement, pour rester maîtres de la situation, le général ADLOFF évoque la place de l’Homme et préconise de s’assurer qu’il soit toujours au centre du dispositif.

CREC Saint-Cyr, le 30 mai 2017.