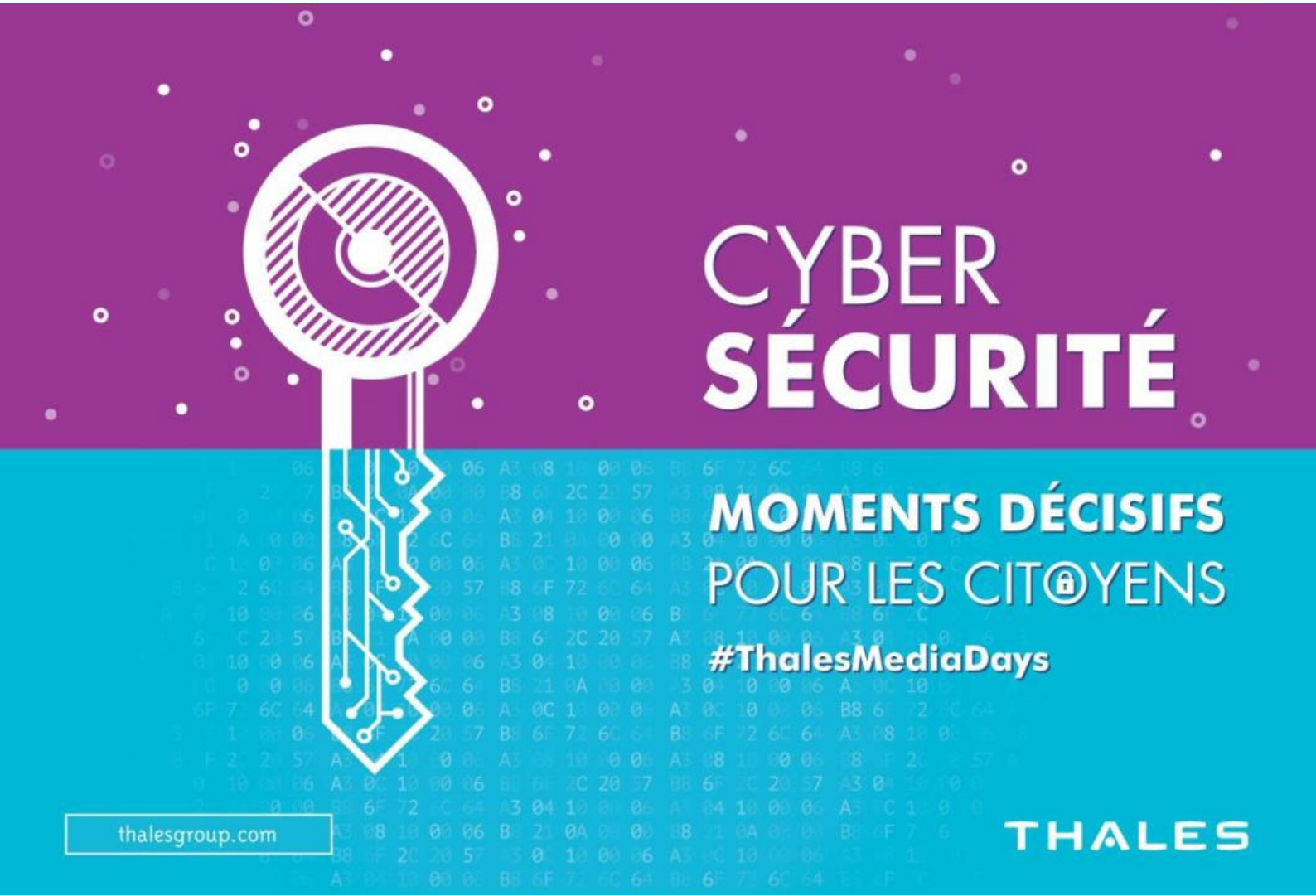
THALES

# Dossier de Presse

## Thales Media Day – Cybersecurité

11 avril 2018



## Sommaire

## A propos de Thales

Ceux qui font avancer le monde s'appuient sur Thales. Nous sommes aux côtés de ceux qui ont de grandes ambitions : rendre le monde meilleur et plus sûr. Riches de la diversité de leurs expertises, de leurs talents, de leurs cultures, nos équipes d'architectes conçoivent un éventail unique de solutions technologiques d'exception, qui rendent demain possible dès aujourd'hui. Du fonds des océans aux profondeurs du cosmos ou du cyberespace, nous aidons nos clients à maîtriser des environnements toujours plus complexes pour prendre des décisions rapides, efficaces, à chaque moment décisif.

Fort de 65 000 collaborateurs dans 56 pays, Thales a réalisé en 2017 un chiffre d'affaires de 15,8 milliards d'euros.

# Cybersécurité : de la confiance dans la cité de demain

**Patrice Caine**

*Président-directeur général, Thales*

Dans la cité de demain, des réseaux de transport intelligents seront interconnectés. Les trajets seront plus sûrs, plus rapides et personnalisés. L'autonomie sera reine, des véhicules individuels aux services de livraisons de nos équipements. En cas d'accident, pompiers, police et secours communiqueront plus rapidement, coordonneront mieux leurs efforts et leurs moyens. Dans la cité de demain, nous effectuerons démarches administratives et transactions bancaires depuis notre smartphone ou notre montre connectée. Nous accéderons de la même façon à notre dossier médical et à une multitude d'informations qui faciliteront notre quotidien.

Mais plus nos villes seront numériques, interconnectées, organisées autour de réseaux vitaux de communications entre personnes ou objets, et plus les risques d'un dysfonctionnement systémique seront importants. La cité de demain sera bâtie sur la confiance numérique que nous placerons en elle. Car elle nous fera passer de réseaux d'échanges fermés à des réseaux ouverts, infiniment plus riches mais aussi plus vulnérables.

Je crois que le développement de la cité numérique se fera parallèlement aux systèmes de cybersécurité que nous pourrons développer et à la mise en place d'un pacte de confiance au bénéfice de la communauté. Les grands acteurs du secteur numérique devront eux aussi répondre à un code de loyauté vis-à-vis de leurs utilisateurs et d'engagements vis-à-vis de principes fondamentaux.

Il leur faudra expliquer pourquoi chaque système est sécurisé, où sont les données, s'assurer de leur fiabilité et surtout préciser l'usage qui en est fait. Le Règlement général européen relatif à la protection des données personnelles (RGPD) deviendra applicable à compter du 25 mai prochain. C'est une opportunité pour tous les opérateurs et fournisseurs de services numériques de forger ce pacte de confiance sur lequel se fonde l'histoire même des échanges.

La cité de demain fera coexister deux espaces, physique et virtuel, qui s'entremêleront en permanence. Chaque citoyen entend profiter de chacun d'eux, souhaitant qu'une nature bien réelle envahisse à nouveau sa ville, tout en restant connecté partout ! Profiter de cette cité connectée sans que ses systèmes puissent porter atteinte à notre identité.

De la même façon que nous nous réapproprions progressivement l'espace urbain, nous sommes suffisamment mûrs pour nous réapproprier l'espace numérique, en définissant collectivement les règles qui formeront la base de nos libertés à venir.

C'est à cette condition que la technologie contribuera à tenir la promesse d'une cité moderne plus humaine, à la fois plus ouverte et plus protectrice.

# Un monde hyperconnecté

**Marc Darmon**

*Directeur général adjoint, Systèmes d'information et de communication sécurisés, Thales*

Ce premier Thales Media Day est pour nous l'occasion de partager notre expertise pour démystifier la cybersécurité et les légendes urbaines développées depuis quelques années. Il est aujourd'hui primordial que l'ensemble des acteurs se mobilise pour sensibiliser notre société hyperconnectée aux impacts de la cybersécurité sur le quotidien de chaque citoyen.

Pour mener ensemble cette révolution numérique en toute sécurité, des solutions existent. L'évolution rapide des technologies offre de nouvelles opportunités qui vont bénéficier à nos clients et nous voulons aider ceux qui nous font confiance à prendre les bonnes décisions en temps réel.

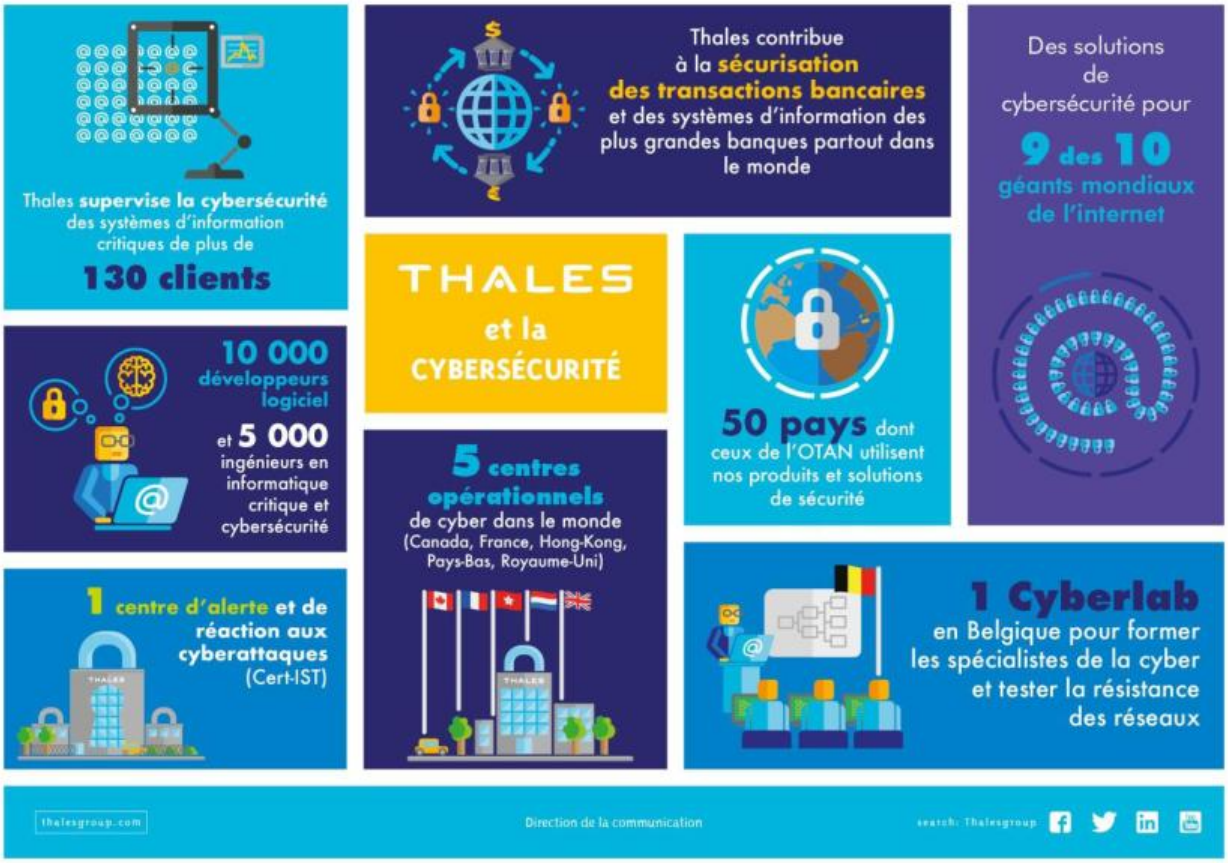
Aujourd'hui, notre monde interconnecté voit cinq évolutions technologiques majeures : le logiciel, les données et l'analytique, la cybersécurité, les prestations « as a service », l'internet des objets et, bien sûr, la migration vers le cloud. Cet engouement pour les environnements nouveaux, et notamment l'IoT, multiplie les surfaces d'attaque et soumet les données à de nouveaux risques qu'il faut contrer par des mesures de sécurité. L'étendue et l'impact croissant des menaces apparaissent très clairement à travers le nombre d'attaques et les niveaux de vulnérabilité.

Grâce à son expertise dans ses 5 grands marchés (aérospatial, espace, transports terrestres, défense et sécurité), Thales a développé au fil des ans des systèmes et solutions cybersécurisés depuis leur conception, « cybersecured by design », pour aider ceux qui font avancer un monde toujours plus connecté. Parce que notre conviction est que la cybersécurité est aujourd'hui devenue l'oxygène de nos sociétés reposant sur l'hyperconnectivité.

Pour répondre à ces enjeux, ces trois dernières années, Thales a investi plus d'un milliard d'euros dans les technologies digitales : Connectivité/IoT, Big Data, Intelligence Artificielle, Cybersécurité. Ces 4 technologies clés du numérique, dans un mouvement de convergence accrue, sont un levier essentiel pour aider nos clients à affronter les évolutions de notre société connectée. Plus encore, c'est l'association de l'ensemble de ces technologies qui est en passe de révolutionner le numérique de demain et de fournir une cybersécurité adaptée à la société moderne.

L'explosion des technologies numériques et de la synergie des technologies du XXIe siècle est un formidable accélérateur pour inventer et développer des produits et solutions d'aujourd'hui, mais dont le monde aura également besoin demain, un monde de données, autonome et immersif.

# Thales et la cybersécurité



# Démonstrations

Sécurité

## Le Cyberlab ou la formation des hackeurs

Alors que le cyberespace est devenu un nouvel espace d'affrontement, la dépendance des entreprises et des Etats avec les systèmes informatiques impose de former et d'entrainer les équipes au même titre que de tester les réseaux et systèmes. En agissant ainsi, les Etats et entreprises préparent les équipes à la gestion d'éventuelles crises, vérifient le niveau de protection des systèmes, et valident les architectures.

Attentif à ce problème, Thales offre un ensemble d'outils et de services pour aider les entreprises et acteurs publics à mieux se préparer et se protéger. Au cœur de ce dispositif, le Cyberlab créé en Belgique par le Groupe permet de reproduire de façon réaliste les réseaux et les systèmes informatiques d'entreprises et d'acteurs publics pour tester leur résistance aux dernières formes de cyberattaques.

Grâce au Cyberlab et à sa plateforme dédiée, le Groupe entend valider le niveau de sécurité des architectures des systèmes d'informations et des données de ses clients, assurer la formation des spécialistes de la cybersécurité dans un environnement représentatif des systèmes réels et accompagner les entreprises dans le développement de produits intégrant la cybersécurité dès leur conception (« secure by design ») en les soumettant aux tests de cybersécurité les plus exigeants.


*Cyberlab de Thales en Belgique © Thales*

Sécurité

## Sonde souveraine : détecter des cyberattaques en temps réel

Les Opérateurs d'Importance Vitale (OIV) sont soumis à des obligations accrues en matière de cybersécurité dans le cadre de la Loi de Programmation Militaire (LPM). Pour protéger leurs systèmes d'informations face aux cyberattaques, il est primordial de détecter les attaques le plus tôt possible et de proposer des solutions de contournement.

Afin de répondre aux nouvelles normes de sécurité, Thales, expert en cybersécurité depuis plus de 40 ans, propose sa sonde de confiance Cybels Sensor, solution modulaire permettant de détecter les cyberattaques sur les systèmes informatiques. La sonde intègre

des algorithmes d'intelligence artificielle qui permettent également d'améliorer les capacités de détection en repérant des intrusions non-connues.

Enrichie par un service de Cyber Threat Intelligence, la sonde intègre un ensemble d'informations fourni par nos sources et analysé par nos équipes. Cette offre complète de cyber-détection est pourvue d'un service, Cybels Decision, fournissant à nos clients une analyse synthétique en temps réel de l'attaque et de son impact sur les réseaux pour prendre la meilleure des décisions à chaque instant.

Sécurité

### Visite virtuelle d'un de nos Centres Opérationnels de Cybersécurité

Face à la croissance des cyberattaques d'origines très variées, sans contrainte géographique et dans un monde massivement interconnecté, se protéger des menaces informatiques est devenu un enjeu capital pour les entreprises. Pour aider les entreprises à faire face aux cybermenaces, Thales s'appuie sur ses centres opérationnels de cybersécurité (CSOC), véritables vigies des infrastructures opérant 24h sur 24, 7jours sur 7.

Présents dans 5 pays (Canada, France, Hong-Kong, Pays-Bas, Royaume-Uni), les centres opérationnels de cybersécurité détectent les menaces en temps réel, analysent et permettent de répondre aux incidents tout en évaluant la conformité des infrastructures en matière de cybersécurité.

Thales vous offre la possibilité, lors des Thales Media Day, d'entrer virtuellement dans le centre hautement sécurisé d'Elancourt qui assure la gestion et la surveillance des systèmes d'information critiques de clients français et internationaux.

Sécurité

### Solutions de Thales pour crypter le cloud et protéger les données

L'adoption généralisée du cloud dans les entreprises et les administrations est un des principaux moteurs de la transformation numérique. Alors que de plus en plus d'entreprises se tournent vers le cloud, celles-ci se heurtent encore à des problèmes de sécurité, déplorant un manque de visibilité sur la façon dont les données sont protégées et une perte de contrôle sur la construction des infrastructures.

Thales offre, en matière d'environnements cloud et de technologies de protection des données multi-cloud, une très large offre de support, utilisant des clés de chiffrement dont l'entreprise conserve le contrôle. Ses solutions avancées de protection des données s'intègrent avec les plateformes des principaux fournisseurs de services dans le cloud, qu'il s'agisse d'Amazon Web Services (AWS), de Google, de Microsoft ou encore de Salesforce, permettant ainsi aux utilisateurs d'ériger de solides barrières de sécurité autour de leurs applications et données sensibles dans le cloud, tout en satisfaisant aux différents critères de conformité et en leur offrant un meilleur contrôle et une plus grande souplesse.

CipherTrust Cloud Key Manager permet aux entreprises soucieuses de respecter les règles de conformité et de faire face aux enjeux de protection des données inhérentes aux environnements multi-cloud de prendre les commandes. Intuitive et conçue sous forme de service, cette offre simplifie la gestion des clés de chiffrement en éliminant le besoin d'architecturer, acheter et déployer du matériel. Au travers d'une interface web facile à utiliser, les entreprises peuvent garder le contrôle de leurs précieuses ressources dans le cloud.

### La cybersécurité pour protéger l'écosystème aéroportuaire

**Sécurité**

Les aéroports sont des lieux de transits à forte concentration de voyageurs. Ces espaces publics de grandes affluences sont devenus des cibles potentielles et il est nécessaire aujourd'hui de les sécuriser efficacement. La sécurité des aéroports met en jeu la protection des infrastructures, des données, des opérations et des personnes. Les aéroports du monde entier doivent faire face à la menace terroriste, protéger leurs sites, par exemple face aux drones, et leurs systèmes d'information face aux cybercriminels.

Afin de lutter efficacement contre les cybermenaces, d'assurer la sécurité des aéroports et permettre au personnel de prendre les meilleures décisions en temps réel, Thales accompagne les opérateurs dans le déploiement de solutions intelligentes au sein des aéroports pour répondre aux exigences les plus rigoureuses en matière de sécurité.

Thales propose un centre de contrôle des opérations aéroportuaires, ou AOCC (Airport Operation Control Centre), mettant à disposition les outils nécessaires pour rendre la gestion de la sécurité et des opérations plus homogènes et plus efficaces au sein du terminal. Le centre de contrôle renforce la vision globale des opérateurs sur les activités de l'aéroport grâce aux informations collectées depuis les différents sous-systèmes. Il permet ainsi une meilleure réactivité du personnel de sécurité en cas de situation d'urgence.

*Centre de contrôle des opérations d'un aéroport © Thales*

### Les OS (systèmes opérationnels) cybersécurisés

**Sécurité**

L'Internet des objets (IoT) est un réseau numérique composé de milliards d'appareils intelligents multifonctionnels et hautement intégrés. Logiciels applicatifs, services cloud et tâches critiques de contrôle doivent collaborer en toute transparence. Le système d'exploitation sous-jacent doit donc jouer un rôle de catalyseur et rassembler capacités IT générales et embarquées.

Dans le monde de l'IoT, les systèmes embarqués ne sont plus isolés, mais font partie d'un réseau mondial. La connectivité les rend vulnérables aux attaques malveillantes et à la manipulation. Selon le rapport sur les menaces liées aux applications mobiles, le nombre d'attaques, sur la seule année 2013, a triplé et devrait continuer de croître de manière régulière.

PikeOS est un système d'exploitation en temps réel basé sur un noyau de séparation offrant une fonctionnalité d'hyperviseur avec plusieurs types de partition pour de nombreux autres systèmes d'exploitation et applications. Il permet à ses utilisateurs de construire des appareils intelligents pour l'Internet des objets conformément aux normes de qualité, de sûreté et de sécurité des différents secteurs industriels.

Dans le contexte de l'Internet des objets, les systèmes embarqués sont confrontés à de nouveaux enjeux : ceux de la sécurité et de la confidentialité. Le système d'exploitation est la première brique à garantir leur protection. L'Internet des objets peut être un lieu dangereux : la protection passe en premier lieu par le système d'exploitation.

**Aéronautique**

### ATM-Cyber : cybersécuriser la gestion du trafic aérien

Malgré les énormes investissements que de nombreux secteurs ont réalisés dans la protection, l'agilité et la détermination des pirates informatiques continuent d'entraîner de graves dommages. Déployer une protection est nécessaire, mais pas suffisant : le moment est venu d'améliorer la résilience avec des capacités de détection, de réaction aux cyberattaques et de rétablissement des opérations. Quels que soient les systèmes, nouveaux ou existants, Thales, au travers de son offre globale de solutions et de services de cybersécurité (ATCyber), renforce les mesures de cybersécurité dans le domaine de la gestion du trafic aérien (ATM).

L'offre ATCyber de Thales fournit tout un éventail de solutions, allant de la protection à la défense active, et apporte aux fournisseurs de services de navigation aérienne des réponses leur permettant de prévenir, gérer et réduire efficacement le cyber-risque.

Par ailleurs, les protocoles de communication de données ATM n'étant pas sécurisés dès la conception, l'utilisation de cyberpasserelles et proxies dédiés à la protection des protocoles ATM est nécessaire.

La solution ATCyber de Thales permet de mettre un frein à l'escalade des cyberattaques dès que des incidents sont détectés. Elle complète l'offre CSOC (centre opérationnel de cybersécurité). Thales fournit aux équipes une formation immersive aux cybermenaces pour faire face aux facteurs humains qui, eux aussi, sont reconnus comme une vulnérabilité.

# Panels de discussion

## Peut-on hacker un avion connecté ?

**Aéronautique**

La numérisation de l'aéronautique constitue évidemment une opportunité : elle permet d'améliorer la performance opérationnelle et de détecter les problèmes potentiellement perturbateurs et d'y répondre de manière plus réactive. Ces technologies rendent notre secteur plus compétitif et efficace. Toutefois, plus de numérisation est également synonyme de nouvelles vulnérabilités, d'une plus grande surface d'attaque et d'une attractivité plus grande pour les pirates. Le débat sera centré sur la question de l'interconnexion croissante entre les constructeurs d'avions, les prestataires de services et les fournisseurs de données, montrant comment cela entraîne une multiplication des vecteurs de menace et fait de l'avion lui-même une future surface d'attaque potentielle.

## Peut-on hacker un satellite ?

**Spatial**

Oui, un satellite peut être piraté, mais il y a peu d'événements connus malgré tout. Un des plus significatifs date de 2005 : des pirates informatiques ayant pris le contrôle d'un satellite pendant une période courte. Depuis, nombres de protection ont été intégrées dans les systèmes de satellites. Par ailleurs, l'architecture des systèmes spatiaux d'aujourd'hui se développe avec plus de dynamique, plus de connectivité. La cybersécurité devient un élément clé pour Thales Alenia Space. *Satellite Iridium® NEXT construit par Thales Alenia Space ©Thales Alenia Space/Master Image Programmes*

## Comment l'industrie ferroviaire anticipe le risque de cyberattaques dans un contexte de digitalisation ?

*Le métro de Dubaï est le plus long métro sans conducteur du monde (70 km) et il constitue la première alternative au transport routier dans le pays © RTA*

Chaque jour, des milliards de personnes prennent le train pour voyager dans d'autres pays ou se déplacer à travers des villes de plus en plus grandes et encombrées. Grâce à la digitalisation, l'automatisation et une connectivité accrue rendront nos trains plus rapides, plus sûrs, plus confortables et plus ponctuels… mais également vulnérables aux cyberattaques. Cela peut générer de graves perturbations dans les transports ferroviaires, donner lieu à des vols de donnés clients et engendrer de graves préjudices économiques. Même la sécurité des passagers est menacée. Dans un tel contexte, protéger nos chemins de fer avec des solutions de cybersécurité avancées est vital.

L'objectif est d'aller bien au-delà de la prévention et la détection de ces attaques mais également de réagir extrêmement rapidement lorsqu'elles se produisent.

**Défense**

### Comment protéger nos armées sur un champ de bataille numérisé ?

20 milliards d'objets connectés en 2020. Alors que dans le monde civil, l'« internet of things » tend vers une croissance exponentielle, l'équivalent militaire existe depuis la numérisation du champ de bataille amorcée dès la fin des années 90. Porteuse d'une révolution technologique pour les systèmes d'armes en permettant la collecte, l'échange, le traitement et le stockage de grands volumes de données, cette hyperconnectivité permettra dans un futur proche le développement de l'intelligence artificielle dans les équipements futurs en l'irrigant de données indispensables à son efficacité. La connectivité totale oblige désormais à intégrer la cybersécurité dès la conception des systèmes comme une dimension structurante et non comme un mal nécessaire.

Au-delà des équipements de défense cyber-sécurisés, il est essentiel de proposer des réflexions, des formations, des entrainements avec l'écosystème de défense. De plus, dans un contexte économique contraint, il est essentiel de mettre en place de nouvelles structures de coopération européennes et internationales, étatiques et industrielles. Thales est notamment engagé dans plusieurs chaires de recherches amont, comme la chaire Cybersécurité et Cyberdéfense Saint-Cyr/Sogeti/Thales.


Enfin, la cybersécurité transforme les métiers des forces armées comme ceux de l'industrie. Mais elle impose également une profonde transformation de la relation armées/industriels. Pour cela, la Direction générale de l'armement (DGA) joue, en France, un rôle prépondérant pour s'assurer de la bonne relation entre grands groupes industriels, start-ups et PME.

### Peut-on hacker une voiture autonome et connectée ?

**Sécurité**

A l'ère du numérique, les constructeurs automobiles intègrent de plus en plus de connectivité aux composants embarqués pour améliorer l'expérience utilisateurs tout en assurant une sécurité maximale pour les citoyens. La transformation numérique et l'évolution de la voiture connectée vers la voiture autonome sont au cœur de cette industrie dynamique, promettant de véritables innovations en cybersécurité sur les années à venir.

Cependant, si les véhiculent connectés offrent de formidables fonctionnalités pour le conducteur, l'évolution des technologies embarquées vers la connectivité, rendent les systèmes informatiques plus vulnérables face aux cyberattaques. La transformation digitale de cette industrie change la donne et impose désormais un besoin vital de cybersécurité de bout-en-bout, depuis les composants électroniques embarqués à tout l'écosystème des voitures et de leurs infrastructures. A ces enjeux s'ajoutent également des questions éthiques et morales auxquelles les acteurs du marché, industriels, chercheurs ou acteurs privés, doivent apporter des réponses pertinentes.

Sécurité

## Le renseignement de la menace : comment pénétrer le cerveau des hackeurs ?

Afin de se protéger efficacement des attaques informatiques, il faut connaitre les techniques et méthodes d'attaque. La Cyber Threat Intelligence répond à cet enjeu essentiel de la pertinence des lignes de défense. Les attaquants ciblent des domaines d'activité, des systèmes informatiques, et il est donc impératif de maintenir un niveau de connaissance de ces menaces pour adapter la détection de chacun de nos clients.

Elle permet de récolter, d'analyser puis de trier toutes les données liées à une cyberattaque, à l'attaquant et à son mode opératoire. Agir en « communauté » est l'un des enjeux majeurs de la Cyber Threat Intelligence pour permettre à chaque acteur d'enrichir ses connaissances sur ces attaques et, ainsi, mieux se protéger.

Aujourd'hui, en partageant leurs analyses des comportements des cybercriminels et des modes opératoires, les équipes de Cyber Threat Intelligence améliorent leurs connaissances des cybermenaces pour renforcer leurs capacités de détection, anticiper les nouveaux risques et lutter ensemble contre les cyberattaques. Pour refléter le fruit du travail de Cyber Threat Intelligence, retour sur le boom des cyberattaques de 2017 : d'abord concentrés sur le vol de données, les hackeurs n'hésitent plus aujourd'hui à faire du sabotage industriel en détruisant les données récoltées, en lançant des *ransomware* ou en activant plusieurs cyberattaques de manière consécutive.

Sécurité

## Que peuvent apporter le Big Data et l'Intelligence artificielle à nos solutions de cybersécurité ?

Le big data et l'intelligence artificielle sont les deux technologies clefs pour une cyber-sécurité active, apprenante et plus intelligente.

Dans la cybersécurité, l'accès aux données est facilité puisque les données sont le trafic sur les réseaux ou son expression résumée à travers les enregistrements (logs) de l'activité des applications et de l'infrastructure. La capacité à traiter ces données massives en temps réel et à y appliquer des technologies d'intelligence artificielle permettra de détecter des attaques y compris les nouvelles attaques, de créer un véritable environnement de confiance numérique dans lequel les comportements anormaux ou inhabituels seront facilement identifiés et dans lequel l'authentification des personnes et des objets sera plus robuste. L'intelligence artificielle permettra aussi par l'automatisation qu'elle apporte de démultiplier et d'augmenter la capacité des experts de la cyber-sécurité, qui sont une ressource rare et pour lesquels la demande ne cesse de croître avec le développement de l'Internet des Objets et le passage à l'échelle qu'il demande.

## Contacts presse


Cédric Leurquin
+33 (0)1 57 77 90 93
+33 (0)6 31 01 53 25
cedric.leurquin@thalesgroup.com


Victoire Chartier
+33 (0)1 57 77 90 22
+33 (0)6 77 04 87 54
victoire.chartier@thalesgroup.com


Giaime Porcu
+33 (0)1 57 77 92 18
+33 (0)6 88 23 84 79
giaime.porcu@thalesgroup.com


Justine Degez
+33 (0)1 57 77 91 71
+33 (0)6 89 34 53 09
justine.degez@thalesgroup.com


Anne-Sophie Malot
+33 (0)1 57 77 89 52
+33 (0)6 31 62 01 60
anne-sophie.malot@thalesgroup.com


Maria Mellouli
+33 (0)1 57 77 84 57
maria.mellouli@thalesgroup.com


Sonia Le Guével
+33 (0)1 57 77 91 60
+33 (0)6 31 31 31 36
sonia.leguevel@thalesgroup.com


Constance Arnoux
+33 (0)1 57 77 91 58
+33 (0)6 44 12 16 35
constance.arnoux@thalesgroup.com


Sandrine Bielecki
+33 (0)4 92 92 70 94
+33 (0)6 80 59 22 04
sandrine.bielecki@thalesaleniaspace.com

Chrystelle Dugimont
+33 (0)4 92 92 74 06
+33 (0)6 25 15 72 93
chrystelle.dugimont@thalesaleniaspace.com