

 **Le magazine
des Ingénieurs de l'Armement**



Sécurité et confiance
NUMÉRIQUES

caia N°92 juin 2010

L'Entreprise de VINCI ENERGIES dédiée à la Défense et à l'Aviation Civile.

Nos Missions :

- ❖ Intégration des Systèmes de Management du Trafic Aérien (ATM / ATC, NAVAIDS...);
- ❖ Déploiement d'Infrastructures de Communication / de Systèmes d'Informations et de Commandement (SIC);
- ❖ Mise en œuvre de solutions de Sécurité et de Protection de sites sensibles;
- ❖ Conceptions d'équipements tactiques;
- ❖ Services de proximité associés.

Nos domaines d'activités :

- ❖ Tous Systèmes d'aide à la Navigation Aérienne, (NAVAIDS, ATM / ATC,...), de Communications (HF, V/UHF, FH, etc...) et de Servitudes associées;
- ❖ Protection périmétrique, Détection Intrusion, Contrôle d'Accès, Vidéo protection, supervision centralisée;
- ❖ Intégration de Systèmes en environnements sensibles (fixes ou mobiles) dans le domaine de la Défense;
- ❖ Services de soutien sur site.



Une capacité de réponses à l'ensemble des problématiques d'Intégration, de Déploiement et de Maintenance des Systèmes Opérationnels installés, en France et à l'étranger

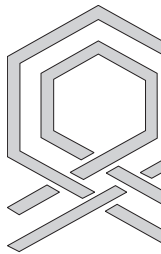
6, Avenue de la Baltique
91140 VILLEBON sur YVETTE

Tél : 01 69 93 80 69

Fax : 01 69 20 05 57

www.gtie-airdefense.fr

Editorial



Chers camarades,

Le présent numéro s'intéresse à la confiance et à la sécurité numériques, domaine qui rentre directement dans notre compétence d'Ingénieurs de l'Armement et nous concerne au quotidien dans nos vies professionnelle comme personnelle.

Jacques Stern, cryptologue de renommée internationale et médaille d'or du CNRS, a accepté de le préfacer.

Le dossier très complet, dont l'élaboration a été dirigée par Yves le Floch, vous exposera des considérations techniques, internationales, géopolitiques et industrielles sur la menace, et son pendant, la confiance numérique.

Mais la sécurité numérique est comme toujours celle de son maillon faible qui en l'occurrence, peut être... nous-même. Raison pour laquelle nous vous proposons une liste de conseils pour protéger vos données, ainsi qu'en encart de ce numéro, le "passport de conseils aux voyageurs" édité par l'Agence nationale de la sécurité des systèmes d'information. En attendant que les projets de puces biométriques implantées sous la peau résolvent le problème, ou au contraire nous précipitent dans un monde beaucoup plus contrôlé... voire apocalyptique.

Notre assemblée générale s'est tenue le 18 mai dernier.

Les choses bougent du côté de notre employeur principal, et nous vous faisons part ci-après des principales nouveautés, comme l'évolution franche de la section "carrières" du Conseil général de l'armement.

Vous retrouverez également vos rubriques habituelles, lectures, carnet pro enrichi des nominations et promotions DGA, histoire, Europe.

Nous profitons de ce numéro pour vous demander votre avis sur notre magazine sous forme d'un petit sondage papier ou en ligne sur notre site www.caia.net. Cinq minutes qui seront précieuses pour votre comité de rédaction.

Bonne lecture et bon avis. 📧

Jérôme de Dinechin
Vice-Président Communications



Le mot du président



Fun, isn't it ? par Philippe Roger, Président de la CAIA

"...Oh Mama, can this really be the end, to be stuck inside of Mobile with the Memphis blues again..." Bob Dylan

Chers camarades,

Ne perdez surtout pas un octet des excellents articles du dossier qui suit !

Il est très instructif, et il montre, ce qui fait plaisir au moment où nous nous inquiétons du maintien des compétences, que le Corps anime une partie importante du domaine traité, de la recherche et de l'enseignement à la conduite des programmes correspondants.

Et appliquez les conseils y contenus. Plus vous vous croyez à l'aise et surfez sur toutes les vagues, plus vous vous approchez de Charybde, de Scylla et du Wipe out. Tombé tout petit dans l'informatique la plus militaire, ayant appris - c'était avant-avant-hier - à ne m'exprimer qu'en ce langage Snobol destiné aux vrais croyants, à ne pas laisser mes bacs de cartes perforées d'IBM 29 plus de 48 heures au guichet du Grand Désordinateur Central (celui dont, pour plus de sûreté, le vocabulaire se limitait à "Fatal Error"), et à me cacher pour programmer aux clés en hexadécimal en face avant d'un ruineux Ramo-Wooldridge 133, je me croyais bien bordé sur la sécurité. Mais voilà que j'achète avant-hier un téléphone-assistant personnel de cette marque qui rappelle le Club Med, et vais pour y transférer les données des quatre générations de PDA successivement acquises chez cet éminent précurseur, me saisissant du câble qui me servait jusques à cette date à les extraire "en toute sécurité" de mon PC.

No way, me dit Help, qui m'enjoint de forwarder le tout sur le Net à G... ou à Y..., ces célèbres sociétés philanthropiques vêtues de probité candide et de lin blanc, qui le downloaderont sur les ondes à mon téléphone, en respectant, foi d'animal et la main sur leur Bible, leur plus entière privacy policy, les règlements fédéraux, and all this sort of things. Pour m'être agréable, me dit Help, elles iront même jusqu'à pick up sans me déranger les nouvelles data apparaissant dans mon téléphone et à en faire part real time à mon PC, d'autant plus fast que leur privacy policy leur interdit de les lire. Drapé dans mes principes de sécurité quadragénaires, et murmurant du Zazie, je m'y refuse, et décide d'attendre que quelqu'un écrive le logiciel de synchro par câble qui va bien, ou que la NSA soit saturée par le stockage des annuaires recueillis sur les ondes.

Eh bien, hier matin, qu'est-ce que je vois dans mon nouveau téléphone, sans avoir rien demandé à personne ? Une copie d'il y a environ trois ans de ma liste de contacts, apparue with no visible means of support par l'intervention du Holy Spirit !

Stuck inside of mobile... 📧

Préface



Préface de Jacques Stern

Professeur à l'Ecole normale supérieure

Président de l'Agence nationale
de la recherche

Médaille d'or du CNRS

Je suis très heureux de présenter ce numéro de la revue des ingénieurs de l'armement consacré à la confiance et à la sécurité numériques, à la fois parce que le sujet exige une réflexion approfondie et parce que les contributions sont uniformément de haut niveau. Elles sont de plus écrites par des spécialistes de talent, dont beaucoup sont des amis de longue date.

Il existe plusieurs façons d'appréhender la sécurité des systèmes d'information. La voie la plus classique est l'approche par fonction : c'est la trilogie fondamentale - intégrité, authenticité, confidentialité - chère aux cryptologues. Toutefois, même en y ajoutant la disponibilité, qui ne relève pas en général des moyens de cryptologie, et la non-répudiation, qui fonde les mécanismes de signature électronique, cette approche ne suffit plus aujourd'hui à rendre compte de la multiplicité et de la diversité des situations qui mettent en jeu la sécurité informatique. Une autre approche, par destination si l'on peut dire, consiste à partir de la menace. Moins structurante, elle permet toutefois de mieux cerner les modes d'emploi attachés à la protection des systèmes. Si l'on se réfère aux différents articles qui suivent, on constate qu'ils ne privilégient aucun des deux points de vue mais au contraire, les adoptent l'un et l'autre, leur permettant ainsi de s'enrichir mutuellement.

La cryptologie, à laquelle j'ai personnellement consacré une large part de mes travaux, a connu dans les trente

dernières années un véritable âge d'or. Après l'invention de la cryptologie asymétrique par Diffie et Hellman et celle du cryptosystème RSA par Rivest, Shamir et Adleman, une large communauté de recherche s'est constituée dans de nombreux pays. L'idée que chiffrement et déchiffrement ne sont pas nécessairement réalisés par des mécanismes essentiellement identiques et ne mettent pas nécessairement en jeu la même clé est devenue une banalité ; les courbes elliptiques sont prêtes à se substituer aux entiers du RSA ; des théories mathématiques du XX^{ème} siècle, notamment le "couplage de Weil", ont même permis de résoudre un problème qui résistait depuis 20 ans, celui de choisir une identité ou une adresse mail comme clé de chiffrement d'un système asymétrique. N'oublions pas que le RSA, pour novateur qu'il ait été, s'appuyait sur des connaissances disponibles au milieu du XVIII^{ème} siècle ! Même le chiffrement conventionnel, un savoir auparavant limité au monde de la défense et du renseignement, a fait l'objet de développements théoriques qui ont conduit à procéder au choix d'un algorithme normalisé, l'AES (Advanced Encryption Standard) au moyen d'une compétition ouverte. La méthode n'a pas si mal réussi puisqu'on la reproduit en ce moment pour le choix d'une fonction d'intégrité !

La doctrine d'emploi en revanche, a peu évolué. Il s'agit toujours d'exécuter les opérations cryptographiques dans un environnement physiquement protégé, de préférer - autant que possible - le matériel au logiciel,

de contrôler la chaîne logistique. Comme toute doctrine, elle a vocation à s'appliquer partout. Elle impose cependant des contraintes d'utilisation, qui peuvent devenir difficilement supportables dans certains contextes et c'est peut-être là que réapparaît l'essence éminemment duale de la spécialité. Les mêmes méthodes sont, dans le monde de l'entreprise ou dans la sphère personnelle, employées avec moins de rigueur dans le respect des règles que si la sécurité nationale est en jeu. Evidemment, il est parfaitement légitime de proportionner la protection des systèmes d'information à la valeur des informations ou des transactions. A condition de ne pas se tromper sur l'analyse du risque et de ne pas ouvrir la voie à des vulnérabilités dont l'exploitation met en danger un domaine bien plus large que celui qu'on anticipait !

Les vulnérabilités et les menaces, hélas, sont légion dans le monde ouvert du WEB 2.0, des réseaux sociaux, du M2M ("communication de machine à machine") et du "cloud computing". Il suffit, pour s'en convaincre, de "surfer sur l'Internet" : ici on rapporte une intrusion ayant conduit à la compromission de dizaines de millions de numéros de cartes de crédit, là on évoque une attaque par déni de service qui rend indisponible tel ou tel serveur, là encore un article de journal explique comment un canal satellite a été piraté ! Ces menaces sont bien entendu détaillées dans les contributions qui suivent, ainsi que les contre mesures qui permettent, dans chaque domaine d'activité numérique, de s'en protéger.

Les difficultés rencontrées sont aussi explicitées. La sécurité numérique doit être assurée à de multiples niveaux physiques et logiques : communications, systèmes d'exploitation, réseaux, applications, sans parler de l'utilisateur final qui est souvent le maillon faible de la chaîne ! Pour être acceptée et générer en fin de compte la confiance, la sécurité doit être - autant que possible - transparente à cet utilisateur final et les procédures qui la mettent en œuvre ne doivent pas lui apparaître inutilement lourdes. Il faut aussi éviter qu'elles n'empiètent sur son "intimité numérique". C'est dire que la tâche n'est pas simple et qu'elle requiert une détermination soutenue. Les bonnes pratiques de la sécurité numérique doivent être présentes dans tout projet dès sa phase de conception et les infrastructures qu'elles requièrent, notamment en termes d'identité numérique, doivent être mises systématiquement en place.

L'universitaire que je suis ne saurait conclure sans évoquer le nécessaire effort d'éducation qui doit accompagner infrastructures et bonnes pratiques de sécurité. Des concepts comme celui de certificat numérique ou de connexion sécurisée doivent devenir, à terme, familiers à tous. La première étape, c'est bien sûr la sensibilisation des *cognoscenti*. C'est bien ce qui est réalisé, de manière remarquablement exhaustive et rigoureuse dans ce numéro !

Bonne lecture. ☺

3 **Editorial**

3 **Le mot du président**

4 **Préface de Jacques Stern**

“Les 15 commandements de l'ordinateur bien protégé”

Tout au long du dossier, vous retrouverez quelques conseils destinés à vous permettre de protéger vos données numériques personnelles et professionnelles.

- 8**
- **Introduction au dossier** *par Yves Le Floch*
 - 10 • **Introduction à la cryptologie. Quels fondements pour la sécurité de nos systèmes numériques ?** *par Guillaume Poupard*
 - 15 • **Interview du directeur général de l'agence nationale de la sécurité des systèmes d'information**
 - 20 • **Les nouveaux enjeux de la sécurisation numérique dans les Armées** *par Marc Sirven*
 - 22 • **Cryptologie et recherche académique** *par Antoine Joux*
 - 24 • **Les dimensions géopolitiques de la sécurité numérique. De la sécurité numérique à la guerre numérique** *par Alain Esterle*
 - 27 • **La guerre des mondes numériques aura bien lieu. Du mythe à la réalité** *par Florent Chabaud*
 - 30 • **Interopérabilité et sécurité des systèmes d'information** *par Jean-Luc Combrisson*
 - 33 • **“High/I/Aie!-Tech”. Quel futur pour la sécurité des systèmes d'information ?** *par Philippe Wolf*
 - 38 • **Quelle protection face aux cybermenaces ? Cyberdéfense : un exemple de solution déployée** *par Christophe Dumas et Stanislas de Maupeou*
 - 42 • **Le passeport biométrique, la sécurité numérique dans votre poche** *par François-Xavier Fraisse*
 - 44 • **Pour une politique industrielle dans le domaine de la sécurité des systèmes d'information** *par Luc Renouil*
 - 46 • **L'Etat du droit pénal** *par Yves Le Floch*
 - 48 • **De la résilience des télécommunications à la sécurité numérique ou comment la révolution numérique bouscule nos critères de sécurité** *par Philippe Duluc*
 - 52 • **Les cartes bancaires et leur sécurité. La version moderne du combat de l'obus et de la cuirasse** *par Pierre Juhen*
 - 54 • **Internet et ses ruptures ?** *par Arnaud Salomon*

55 **Publi-reportage**

- Alcatel Lucent • CCI du Var • Continental • EADS

62 **Europe**

- Trois présidents, un visage *par Michel Clamen*

64 **Libre Propos**

- De la mission rayonnement de la DMA à la section carrière du CGARm... *par Daniel Reydellet*

66 AG

- Une AG sous haute sécurité... *par Philippe Roger*

67 Vie de la CAIA

- Deux présidents et deux trésoriers pour une AG *par Julie Morvant*

68 Technique

- SCORPION : Une évolution majeure de la conduite de projet dans le domaine terrestre *par Jérôme Lemaire*

71 Management

- Quel genre de lecteur êtes-vous ? Petit sondage pour nous aider à mieux manager notre magazine

74 Histoire

- Enigma et les progrès de la cryptanalyse *par Daniel Jouan*

79 Lu pour vous

- Mission d'un cryptologue français en Russie (1916) *d'Henry Olivari*
- Histoire des codes secrets *de Simon Singh*

80 Promotions et décorations

- Lettre d'information trimestrielle des officiers des corps de l'armement (mai 2010)

84 Lu au JO

85 Carnet professionnel

Rédacteur en chef : Jérôme de Dinechin **Rédacteur en chef délégué** : Yves Le Floch **Comité de rédaction** : Arnaud Salomon, Michel Clamen, Dominique Luzeaux, Marc Mouly, Xavier Lebacq, Philippe Gassmann, Daniel Jouan, Louis Le Pivain, René Neyret, Joël Rosenberg, Sarma Gadindra **Secrétaire** : Aïda Rosemain
Édition et régie publicitaire : S.N.E **Création graphique** : La Clique

Sécurité et confiance numériques

Introduction au dossier



par **Yves Le Floch**

Ingénieur en chef de l'armement

Conseiller du secrétaire général de la défense et de la sécurité nationale

Avant de rejoindre les services du Premier ministre, Yves Le Floch a été responsable du soutien logistique intégré et de l'intelligence économique à la DGA. Il a été chargé de la réorganisation de la fonction RH et responsable de programmes d'armement. Il a travaillé auprès du délégué à l'information et à la communication de la Défense ainsi qu'au Centre d'Analyse et de Prévision du Quai d'Orsay.

Le projet Ultra, nom de code de l'immense effort britannique pour casser les codes secrets allemands pendant la Seconde Guerre mondiale, a certainement raccourci la guerre de 3 ans. Compte tenu de ce qu'il révélait des capacités alliées, il est resté totalement secret pendant la guerre et durant les trente années qui ont suivi la victoire des alliés. La cryptanalyse de la machine Enigma, qui protégeait les communications militaires de l'Axe, ou du code Lorenz, qui chiffrait les échanges des dirigeants nazis, n'ont ainsi été révélés qu'en 1974.

Comme le montre cet exemple historique, de la sécurité de l'information peut dépendre le

cours de l'histoire. Ou bien le succès d'une opération militaire, la réussite d'une négociation diplomatique, l'obtention d'un contrat stratégique...

Avec l'arrivée des ordinateurs et des réseaux électroniques, les techniques autrefois utilisées par les diplomates et les militaires se sont développées et ont trouvé place dans la vie de tous les jours. Les enjeux associés n'ont fait que croître en importance, en ajoutant aux secrets des États et des armées le secret industriel et commercial et la protection des données personnelles. Ainsi, la cryptographie à clés publiques protège

chaque jour nos échanges sur Internet, la sécurité informatique défend nos ordinateurs personnels et professionnels. Nos communications mobiles, nos badges sans contact, nos paiements par carte à puce et nos transactions bancaires sont chiffrés. Mais comme pour la cryptographie traditionnelle de l'époque du projet Ultra, toutes ces techniques ont leurs limites ou leurs failles.

Les attaquants se sont eux aussi multipliés dans le monde. Les - nombreux - cryptanalystes de quelques grandes agences de renseignement poursuivent plus que jamais leurs travaux dans l'obscurité du

Les principaux organismes

Dans le domaine de la sécurité des systèmes d'information (SSI), et plus généralement de la cyberdéfense, l'autorité nationale interministérielle est l'agence nationale de la sécurité des systèmes d'information (ANSSI) qui relève du Premier ministre et est placée sous l'autorité directe du secrétaire général de la défense et de la sécurité nationale (SGDSN). Créée en 2009, l'ANSSI est l'héritière d'une longue série d'organismes, souvent appelés "service du chiffre", qui ont été chargés d'assurer la sécurité des informations sensibles de l'État tout au long du XX^{ème} siècle. Dans le domaine du chiffrement gouvernemental, c'est la DGA qui développe les algorithmes de chiffrement et qui assure la maîtrise d'ouvrage des produits de très haute sécurité ; elle assure elle-même l'évaluation des produits de sécurité gouvernementaux. L'agrément des produits, indispensable à leur utilisation pour de l'information classifiée, est prononcé par l'ANSSI.

En Allemagne, l'autorité nationale est l'office fédéral de la sécurité de l'information, le BSI selon son sigle allemand, qui dépend du ministère de l'intérieur. Au Royaume-Uni, plusieurs services se partagent le rôle d'autorité nationale, l'autorité technique étant le Communications-Electronics Security Group (CESG), qui dépend du Government Communications Headquarters, service de renseignement technique britannique. La situation est semblable aux États-Unis où l'autorité technique nationale relève de la National Security Agency (NSA), service de renseignement technique. Au niveau européen, l'agence européenne de la sécurité des systèmes d'information et des réseaux, connue sous son sigle anglais ENISA, a été créée en 2004-2005 pour soutenir l'action de la commission européenne, des états et des acteurs européens dans le domaine de la SSI.

L'antivirus quotidiennement tu tiendras à jour

La mise à jour de l'antivirus doit être activée automatiquement avec un rythme au moins quotidien. S'il représente une certaine protection contre les attaques les plus courantes qui circulent sur l'Internet, et est indispensable à ce titre, l'antivirus ne protège généralement pas contre les attaques plus sophistiquées.



Des PME à côté de grands groupes industriels

L'offre en matière de produits de sécurité est traditionnellement segmentée de la façon suivante :

- anti-virus, protection contre les codes malveillants ;
- pare-feu (firewall) ;
- détection d'intrusion ;
- effacement sécurisé de données ;
- administration et supervision de la sécurité ;
- identification, authentification et contrôle d'accès ;
- communication sécurisée ;
- messagerie sécurisée ;
- stockage sécurisé ;
- matériel et logiciel embarqué.

Quelques acteurs français bien connus du monde de la défense sont intégrateurs de systèmes de sécurité ou vendeurs de produits gouvernementaux de souveraineté, "agrés" pour le classifié de défense : BERTIN, BULL, CS, EADS, SAGEM, THALES. Ils peuvent être leaders au plan européen, voire mondial, dans divers domaines de la sécurité. Des prestataires de services de sécurité, parfois opérateurs de communications électroniques, proposent par ailleurs des offres de service en matière de sécurité de l'information.

A leurs côtés, des PME se sont spécialisées dans certaines niches et offrent des solutions originales, notamment pour sécuriser le monde de l'IP (Internet Protocol). Grâce à leur capacité d'innovation et leur réactivité, elles arrivent à tirer leur épingle du jeu avec des offres de produits, dont certains bénéficient de labels délivrés par l'ANSSI, tels que des pare-feu, des solutions de chiffrement, des clés USB sécurisées, des solutions de signature et d'identification, des logiciels de confiance... Ces produits représentent pour les PME françaises concernées un chiffre d'affaires cumulé estimé à 200 M€, montant faible au regard du marché mondial. L'offre française devrait se renforcer avec l'équipement progressif de l'administration, et sans doute d'entreprises soucieuses de la protection de leurs données, en produits de sécurité labellisés.

On peut néanmoins s'inquiéter de l'intérêt croissant que les investisseurs étrangers portent aux PME françaises sensibles depuis quelques années : la prise de contrôle par des capitaux étrangers est certes, dans certains cas, soumise à autorisation de l'administration, mais il n'en reste pas moins que cette tendance peut entraîner des conséquences en matière de souveraineté.

secret d'Etat ; nous ne saurons rien de leurs moyens ni de leurs résultats. Mais avec l'Internet et les publications scientifiques, certaines de leurs techniques sont désormais accessibles à un large public et donnent lieu à des réalisations décrites en ligne qui peuvent mettre en danger vos échanges. Considérez ainsi que vos liaisons wi-fi, vos badges sans contact, vos échanges sur Internet et vos communications GSM peuvent être vulnérables à des "curieux" déterminés. En matière de sécurité informatique, les failles sont multiples et rares sont les ordinateurs réellement protégés contre les attaquants informatiques habiles, qui sont légion. L'époque du hacker adolescent génial qui se vantait de ses intrusions inoffensives est révolue. L'intrusion dans les réseaux et les systèmes informatiques, l'atteinte aux échanges électroniques privés sont désormais devenues de véritables industries qui, parfois de mèche avec des services étrangers, brassent de grandes quantités d'argent et font appel à d'excellents

professionnels : les pirates du net écumant en permanence les réseaux à des fins crapuleuses, d'espionnage ou de rétorsion. Il n'est plus un conflit entre états ou entre communautés qui ne se double de son pendant numérique.

Dans ce monde numérique dangereux, nous dépendons de plus en plus des réseaux électroniques et de leur sécurité. En tant que personne d'abord, qui confie au cyberspace ses données privées, son argent et ses centres d'intérêt personnels. En tant qu'acteur économique ensuite, car les entreprises ne savent plus aujourd'hui se passer de réseaux électroniques fiables. En tant que citoyen enfin, qui dépend de la capacité des services publics à garantir, y compris sur les réseaux, la sécurité de leurs opérations et de leurs activités.

Les grands états ont désormais pris conscience des enjeux. En France, le Livre blanc sur la défense et la sécurité nationale publié en 2008 annonce la multiplication des attaques informatiques, parfois de grande

ampleur. Il estime que des attaques visant la France seront très probablement d'origine étatique ou para-étatique ; certaines seront dissimulées, d'autres pourront être massives. Dans ce contexte, le Gouvernement a décidé un renforcement très rapide des capacités nationales de défense informatique. L'agence nationale de la sécurité des systèmes d'information (ANSSI), créée en juillet 2009, en est le fer de lance et doit doubler ses effectifs d'ici à 2012. Les administrations, les armées, les services publics, les grandes entreprises, les opérateurs sont des cibles et doivent, chacun à sa mesure, mettre en place la défense informatique de leurs réseaux et systèmes.

Ce dossier fournit de nombreux conseils de sécurité informatique directement utilisables. Il vous offre surtout un éclairage d'ensemble sur un sujet qui est aujourd'hui au cœur de la sécurité des états, des entreprises et des citoyens.



Sécurité et confiance numériques

Introduction à la cryptologie

Quels fondements pour la sécurité de nos systèmes numériques ?



par **Guillaume Poupard**

Ingénieur en chef de l'armement

X92, docteur en cryptologie, ancien responsable du laboratoire de cryptologie de l'ANSSI, actuellement conseiller technique au sein du ministère de la Défense

Bien que plusieurs fois millénaire, la cryptologie définit les fondements même de la sécurité de nos très modernes systèmes d'information. Inspirée à la fois par les mathématiques, l'informatique et la théorie de l'information, cette discipline a connu au cours du dernier demi-siècle une évolution sans précédent, à la hauteur des enjeux modernes de sécurisation que nous nous proposons de parcourir.

1949 : après des siècles d'usage militaire et diplomatique de la cryptographie, Claude SHANNON publie ce qui aurait pu être un point final à la recherche en cryptologie¹ en confirmant qu'il existe des systèmes de chiffrement parfaitement sûrs mais que ces derniers sont tous inutilisables en pratique ! Pourtant, 60 ans plus tard, les mécanismes cryptographiques, bien que discrets, sont devenus omniprésents et sécuriseront à terme l'ensemble de nos communications téléphoniques ou électroniques, de nos transactions bancaires, de nos données personnelles... en un mot toutes les informations numériques, qu'elles soient stockées ou transmises.

Pour comprendre cet apparent paradoxe, revenons au besoin initial, d'origine millénaire, qui est d'échanger des

informations en garantissant leur confidentialité malgré les risques d'interception par des tiers. Les procédés de chiffrement² permettent de transformer de manière réversible des données afin de les rendre inintelligibles. Les méthodes sont multiples mais reposent toutes sur deux techniques élémentaires consistant soit à permuter les symboles, soit à en changer la représentation, typiquement en substituant des caractères par d'autres. Partant de cette observation, il est tentant de concevoir des méthodes les plus alambiquées possibles et de les garder secrètes. Cette démarche est naturelle mais l'Histoire nous montre qu'il est bien difficile de protéger une méthode de chiffrement, qu'il s'agisse, pour ne citer que deux exemples, de la machine allemande ENIGMA utilisée lors de la

Seconde Guerre mondiale ou de l'algorithme A5 de chiffrement des communications radio du GSM. L'approche moderne s'appuie donc sur le principe attribué à Antoine KERCKHOFFS selon lequel la sécurité ne doit pas reposer sur la confidentialité des méthodes de chiffrement. Par conséquent tout le secret doit être concentré dans les clés, ces éléments numériques de quelques dizaines à quelques centaines d'octets choisis de manière essentiellement aléatoire. Un second principe majeur en matière de conception d'algorithmes de chiffrement est de garder à l'esprit qu'il s'agit d'une activité délicate qui doit être menée rationnellement en se gardant bien de penser qu'abus de complexité rime nécessairement avec sécurité. Historiquement, tous les systèmes conçus

En administrateur jamais ne navigueras

Au quotidien, l'ordinateur doit être utilisé en mode de simple "utilisateur", la session "administrateur" n'étant utilisée que pour certaines opérations particulières telles que l'installation de logiciels. On limite ainsi fortement les risques d'infection ou de compromission de l'ordinateur car de nombreux logiciels malveillants ne peuvent s'installer sur la machine si l'utilisateur n'a pas de privilège d'administration.



avant la Seconde Guerre mondiale ont été cryptanalysés. De plus, l'intense recherche académique qui s'est développée depuis la fin des années 1970 a permis de découvrir des méthodes d'attaque très subtiles qui, combinées à une puissance de calcul exponentiellement croissante, rend délicate la tâche du cryptographe. L'état de l'art semble cependant se consolider et l'on peut aujourd'hui avoir raisonnablement confiance dans les algorithmes de dernière génération à l'image du standard commercial américain AES. Cet algorithme utilise des clés secrètes de 128, 192 ou 256 bits et permet, toujours au moyen d'un enchaînement habile d'opérations de substitution et de permutation, le chiffrement de blocs de 128 bits.

A ce stade, arrêtons-nous un instant sur l'idée reçue selon laquelle "il est toujours possible de casser un code secret à condition d'y mettre les moyens". Cette idée est légitimée par l'existence d'une attaque générique très simple qui s'applique à tous les algorithmes de chiffrement utilisant des clés secrètes de taille fixe et qui consiste à tester l'ensemble des clés possibles ; si les clés sont de taille fixe, le nombre d'essais est fini et l'énumération est mathématiquement possible. Une telle stratégie a d'ailleurs été mise en œuvre avec succès pour attaquer l'algorithme DES, prédécesseur de l'AES. Il convient cependant de remarquer que le nombre d'essais à réaliser croît exponentiellement avec la taille des clés. Là où le DES dispose de clés de 56 bits³, taille au demeurant suspecte aux yeux de n'importe quel informaticien, l'AES utilise des clés de 128, 192 ou 256 bits. On peut longuement s'interroger sur la faisabilité d'une recherche exhaustive sur des clés de 128 bits⁴, recherche aujourd'hui certainement hors de portée y compris pour les agences de renseignement les plus puissantes. Par contre pour des clés de 256 bits le doute

n'est pas permis, même pour les plus paranoïaques d'entre nous, car énumérer l'ensemble des clés de 256 bits revient à réaliser un nombre de tests comparable au nombre de particules de l'univers ce qui, convenons-en, est une bonne approximation de l'infini ! Nous tenons là l'explication du paradoxe lié au résultat de Shannon qui indique que pour chiffrer de manière parfaitement sûre il faut utiliser des clés de même taille que les données à protéger, ce qui réduit considérablement l'intérêt de la méthode. Utiliser un algorithme tel qu'AES avec des clés de taille fixe, même de 256 bits, n'est donc pas à proprement parler "parfaitement sûr" mais seulement "calculatoirement sûr" face aux attaques génériques de recherche exhaustive sur les clés,... ce qui est finalement bien suffisant en pratique, même pour les applications les plus sensibles.

En résumé, la situation est plutôt positive puisque l'on dispose aujourd'hui d'algorithmes de chiffrement de qualité qui devraient résister, y compris dans le futur, aux tentatives de cryptanalyse. Une certaine prudence est bien entendu de rigueur puisque rien ne prouve de manière irréfutable la sécurité de ces mécanismes mais l'avantage semble avoir durablement basculé du camp des cryptanalystes dans celui des cryptographes. Tous les problèmes sont-ils pour autant résolus ? Certainement pas ! Citons une seule difficulté majeure : toute la cryptologie classique repose sur l'hypothèse qu'émetteurs et destinataires disposent de secrets communs, les clés qui servent à la fois au chiffrement et au déchiffrement. Si dans un contexte militaire ou diplomatique il est heureusement possible de mettre en place des mesures organisationnelles permettant une distribution sécurisée des clés secrètes aux bonnes personnes, de nombreuses applications modernes de la cryptographie

se heurtent à la difficulté du partage de ces clés. Un exemple illustre ce propos : si l'on souhaite chiffrer ses échanges avec un site de commerce en ligne sur Internet, par exemple pour transmettre ses identifiants bancaires, comment partager un secret initial avec un tel interlocuteur que l'on ne connaît même pas véritablement ? Toutes les solutions naïves qui consistent à s'envoyer des bouts de secret sont inefficaces puisqu'un attaquant qui écouterait la communication pourrait en déduire lui aussi la clé secrète ainsi définie.

“Historiquement, tous les systèmes conçus avant la Seconde Guerre mondiale ont été cryptanalysés”

La solution à ce problème a été proposée en 1976 par Whitfield DIFFIE et Martin HELLMAN qui ont observé que rien n'impose que les opérations réciproques de chiffrement et de déchiffrement soient réalisées avec une seule et même clé. Mieux, si les clés sont distinctes, il est très tentant de rendre publique la clé de chiffrement et de ne garder secrète que la clé de déchiffrement. Le paradigme du chiffrement asymétrique est ainsi posé : chacun dispose de deux clés, une clé publique largement diffusée et qui permet à n'importe qui de chiffrer des messages à son attention et une clé privée qui est gardée confidentielle et qui permet de déchiffrer les messages. Une telle approche est remarquable car elle résout le problème du partage initial de secret sans nécessiter de mesure organisationnelle. Toute la difficulté

Sécurité et confiance numériques

est d'implémenter dans un monde numérique une telle idée car, bien que les clés publiques et privées soient évidemment intimement liées, il doit notamment être impossible à partir de la clé publique de retrouver la clé privée. La première solution a rapidement été proposée par Ronald RIVEST, Adi SHAMIR et Leonard ADLEMAN qui ont proposé le système devenu célèbre

“L’avantage semble avoir durablement basculé du camp des cryptanalystes dans celui des cryptographes”

sous leurs initiales : RSA. Ce système, comme tous les systèmes asymétriques, repose sur un problème algorithmiquement difficile qui, sans être insoluble, nécessite lorsqu'il est correctement dimensionné une puissance de calcul inaccessible. Dans le cas de RSA, il s'agit du problème de la factorisation d'entiers en facteurs premiers : il est relativement facile de générer deux nombres premiers (i.e. divisibles uniquement par 1 et par eux-mêmes) de taille fixée puis de les multiplier entre eux pour obtenir un entier composé. À l'inverse, retrouver ces deux nombres premiers à partir du résultat de leur multiplication est un problème mathématiquement bien défini mais qui, en l'état des connaissances, nécessite une capacité de calcul qui croît très rapidement avec la taille des nombres manipulés. À titre d'illustration le record public de factorisation a récemment été réalisé sur un entier de 232 chiffres décimaux, soit 768 bits.

L'intérêt d'un système comme RSA est double : d'une part il permet d'adresser fonctionnellement un très grand nombre de situations et notamment de sécuriser les échanges entre correspondants sans partage initial d'un secret commun. D'autre part, la sécurité de ce système repose sur un problème algorithmique précisément identifié et il est possible de démontrer rigoureusement qu'il n'y a pas de failles de sécurité autres que celles éventuellement liées à ce problème de base. Par contre, si des progrès algorithmiques majeurs sont réalisés, la sécurité de tout le système s'effondrera. Or, l'histoire récente des mathématiques montre que certains problèmes, notamment en théorie des nombres, sont parfois résolus après des siècles de recherche. De plus, autant la mise au point de supercalculateurs est complexe et coûteuse, autant la découverte de procédés algorithmiques révolutionnaires peut être faite par des individus brillants sans moyens matériels particuliers... La cryptographie asymétrique est donc une découverte majeure qui, combinée à des briques cryptographiques plus conventionnelles comme l'AES, a permis une explosion des usages de la cryptographie. Elle repose cependant exclusivement sur quelques problèmes que l'on espère difficiles à résoudre, problèmes au demeurant peu nombreux et majoritairement issus de la théorie des nombres, les plus prometteurs étant liés à des objets mathématiques appelés “courbes elliptiques”.

En offrant des méthodes robustes de chiffrement et de gestion des clés associées, la cryptographie moderne propose des briques essentielles à la sécurisation des systèmes d'information et de communication, qu'ils soient civils ou

militaires, gouvernementaux ou commerciaux. Mais la cryptologie apporte bien plus car au-delà des besoins de confidentialité, il apparaît de plus en plus nécessaire d'assurer d'autres services de sécurité comme l'intégrité des données transmises ou bien l'authenticité de leur origine, ce qui ouvre le champ aux applications de signatures électroniques. Une signature est un élément d'authentification qui doit pouvoir être généré uniquement par le signataire légitime mais idéalement vérifiable par n'importe qui, d'où l'idée d'employer une clé privée pour signer et la clé publique associée pour vérifier la validité de la signature. Il est ainsi possible d'authentifier n'importe quel élément numérique, la sécurité globale reposant d'une part sur le problème algorithmique sous-jacent, comme pour le chiffrement asymétrique, et d'autre part sur une bonne gestion des clés. Ce dernier point est fondamental car un tel système ne vaut que si les clés privées sont correctement protégées et si les clés publiques sont elles-

“La cryptographie asymétrique est une découverte majeure qui a permis une explosion des usages de la cryptographie”

mêmes authentifiées. Idéalement, le premier point se résout techniquement au moyen d'éléments tels que les cartes à puces capables non seulement de stocker les clés



Cryptologie quantique et mécanique quantique

Il convient de distinguer la “cryptographie quantique” du “calcul quantique”, deux notions qui n’ont rien à voir. La cryptographie quantique est une nouvelle approche de la problématique de la mise en accord de clé qui ne consiste pas à reposer sur des problèmes algorithmiques mais plutôt sur les propriétés physiques du canal de transmission et sur la possibilité de détecter d’éventuelles interceptions. Le concept est maîtrisé, son implémentation progresse et la question est aujourd’hui de définir quelles applications nécessitent une telle approche plutôt qu’une démarche cryptographique plus classique.

Le calcul quantique est d’une toute autre envergure et représente une véritable révolution de la notion même de calcul. Pour faire simple, un ordinateur quantique utilise la notion de superposition d’état pour réaliser une sorte de parallélisme massif. La faisabilité d’un tel instrument est encore sujette à caution mais les avancées de ces dernières années tendent à montrer qu’il sera probablement possible de le réaliser un jour. Dans ce cas les conséquences sur les mécanismes conventionnels tel qu’AES seraient en pratique négligeables à condition de favoriser les plus grandes tailles de clés prévues par la norme, soit 256 bits. Par contre, celles pesant sur une part importante de la cryptographie asymétrique seraient simplement catastrophiques puisque des algorithmes efficaces de factorisation “quantique” sont d’ores et déjà bien connus. La question est donc de savoir d’une part quand un tel équipement sera disponible et d’autre part qui y aura accès. Entre catastrophisme et déni de réalité, il convient donc d’adopter une position lucide sur les véritables menaces qui pèsent sur nos systèmes numériques.

privées mais également d’effectuer les calculs les impliquant de manière à ne jamais avoir à révéler leurs secrets. Le second point est traité par une utilisation récursive du mécanisme de signature : pour authentifier une clé publique, i.e. garantir qu’elle appartient bien à un individu donné, il suffit qu’une autorité signe un certificat numérique qui l’atteste. Afin de vérifier la validité d’un tel certificat, il faut que la clé publique de cette autorité soit elle-même authentifiée, d’où la nécessité de la faire certifier à son tour par une autorité supérieure, et ainsi de suite. Finalement, on aboutit à une autorité dite racine dont on doit connaître la clé publique. Ce point de départ de la confiance peut être inscrit dans des cartes à puce ou bien dans les navigateurs Internet, ou bien encore publié au journal officiel³ ! Une telle construction, appelée IGC pour infrastructure de gestion

de clé, est réalisable mais complexe à mettre en œuvre à grande échelle, surtout si l’on souhaite pouvoir révoquer des certificats, i.e. en annuler la validité après émission. Généralement invisible aux yeux des utilisateurs, la cryptologie apporte donc les éléments fondateurs de la sécurité de tout système numérique. Elle est indispensable mais doit être correctement définie, implémentée et combinée à d’autres mécanismes techniques et démarches organisationnelles afin de garantir globalement une sécurité à la hauteur des enjeux modernes. ☞

¹La cryptologie, élégamment définie comme la science du secret par Jacques STERN, se décompose en deux activités : la cryptographie qui conçoit les mécanismes et la cryptanalyse qui tente de les attaquer.

²Le vocabulaire français désigne par chiffrement

l’opération de transformation de données claires en messages inintelligibles, de déchiffrement l’opération inverse lorsque l’on dispose des éléments secrets permettant de le faire et de décryptement cette même opération lorsque l’on n’a pas les clés. Tout autre terme tel que cryptage ou encryptage est a priori incorrect.

³Enumérer toutes les clés de 56 bits nécessite par exemple 10 000 processeurs effectuant chacun 10 millions de tests à la seconde pendant 10 jours.

⁴Enumérer toutes les clés de 128 bits nécessiterait 1000 milliards de processeurs effectuant chacun un milliard de tests à la seconde pendant 15 milliards d’années.

⁵Avis relatif aux certificats électroniques de l’autorité de certification racine de l’administration française, dits “certificats IGC/A”, Journal officiel du 17 février 2007, pp 126-128.

Dictao est l'éditeur logiciel de référence dans le domaine de l'authentification forte, de la signature électronique et de l'archivage sécurisé.

Dictao



Produits certifiés
au niveau EAL3+ par l'ANSSI

Produits référencés
au catalogue GAIA

Sécurité et confiance des applications dématérialisées

Authentification forte

Pour qu'une personne puisse prouver son identité, avec un moyen adapté à l'usage et au niveau de risque (mot de passe à usage unique, certificat sur carte à puce, token, etc.)

Signature électronique et preuve

Pour qu'une personne puisse signifier son engagement électroniquement (la signature électronique remplace la signature manuscrite)

Coffre-fort électronique

Pour qu'une organisation puisse conserver des données de manière très sécurisée, enregistrer des traces et garantir un archivage à vocation probante



Nos produits sont éprouvés dans la **sphère publique et la Défense** (archivage sécurisé, téléprocédures), le secteur **bancaire** (authentification des clients entreprises ou particuliers, signature électronique des ordres de virement, souscription de contrats en ligne, etc.), l'**industrie** (dématérialisation des appels d'offres, des commandes, des factures, etc.).



Sécurité et confiance numériques



Interview de Patrick Pailloux Ingénieur général des mines Directeur Général de l'agence nationale de la sécurité des systèmes d'information

La CAIA : quelles sont les priorités qui vous ont été fixées lors de la création de l'agence l'an dernier ?

Patrick Pailloux : Comme l'indique le Livre blanc sur la défense et la sécurité nationale, la probabilité d'une attaque informatique majeure contre les infrastructures nationales dans années à venir est très forte et c'est dans cette perspective que le Gouvernement a créé l'ANSSI en juillet 2009. Celle-ci doit mettre en œuvre un véritable centre opérationnel de cyberdéfense incluant une capacité de détection des attaques informatiques sur les réseaux les plus sensibles de l'administration. Elle est chargée de doter l'État de moyens de communication sécurisés et résilients. Elle doit développer la sécurité des réseaux de communications électroniques liés aux infrastructures critiques du pays, et notamment la résilience de l'internet. L'agence est également chargée de sensibiliser et d'informer les acteurs économiques et le grand public sur les risques dans le cyberspace ainsi que sur la manière de s'en protéger.

La CAIA : quelles sont les attaques informatiques que vous observez ?

Patrick Pailloux : Les attaques les plus fréquentes sont le phishing, c'est-à-dire des courriels trompeurs qui visent à vous faire dévoiler vos identifiants et mots de passe, et les défigurations de sites web. Au-delà de ces attaques courantes, il existe deux grands types de menaces : d'une part l'attaque en déni de service, c'est-à-dire le blocage du système d'information, qu'il s'agisse d'un site web, de l'informatique d'une institution ou d'un pays ; d'autre part l'intrusion discrète, difficile à détecter et très efficace pour dérober en masse les données confidentielle de l'organisme visé.

Un grand nombre de ces attaques supposent la prise de contrôle d'ordinateurs à distance, à l'insu de l'utilisateur, afin de voler les données détenues dans la machine visée et d'intégrer celle-ci à un "botnet", un réseau d'ordinateurs compromis. Cela touche malheureusement toutes les strates de la société - État, grandes entreprises, PME, particuliers - dans tous les domaines. La méthode est souvent plus ou moins la même :

une clé USB infectée ou un courriel avec une pièce jointe piégée.

La CAIA : pour ce qui concerne votre première priorité, la détection des attaques informatiques, comment pouvez-vous vous y prendre ?

Patrick Pailloux : Notre centre opérationnel assure d'ores et déjà, 24 heures sur 24 et 365 jours par an, une activité de veille, d'alerte et de réaction sur les incidents et les vulnérabilités des systèmes d'information. Ce service de cyberdéfense est à même de détecter les attaques majeures et d'y répondre, en coordination avec les forces de sécurité. Nous le développons très activement, en liaison avec les ministères que nous protégeons, pour être capables de détecter les attaques les plus insidieuses. Pour ceci, le facteur essentiel est de connaître en temps réel les menaces et les voies d'attaques (vulnérabilités des systèmes, adresses IP des machines attaquantes, courriels et fichiers piégés, sites malveillants...). Comme les concepteurs d'antivirus, nous devons adapter en temps

Sécurité et confiance numériques

réel nos outils à la menace ; mais nous ne travaillons pas uniquement sur les signatures des fichiers malveillants mais sur divers paramètres nous permettant de reconnaître une attaque lorsqu'elle intervient ou lorsqu'elle produit ses effets.

Les relations internationales sont naturellement essentielles en la matière et nous les développons énormément, au niveau bilatéral comme multilatéral. A l'échelle européenne, par exemple, nous collaborons avec l'ENISA, l'agence européenne chargée de la sécurité des réseaux et des systèmes d'information. Tous les pays sont confrontés aux mêmes problèmes que nous et ont intérêt à coopérer. C'est ainsi que le botnet "Mariposa" a pu être démantelé. Ce réseau regroupait plus de 12 millions d'ordinateurs infectés, appartenant à des entreprises, des administrations et des particuliers dans 190 pays.

Nous disposons par ailleurs d'une équipe d'audit qui inspecte régulièrement les systèmes d'information de l'État, afin d'aider les administrations à améliorer la sécurité des dispositifs opérationnels, notamment les plus sensibles d'entre eux.

La CAIA : Avez-vous déjà recensé des attaques contre des infrastructures de l'État ?

Patrick Pailloux : Bien sûr, nous traitons au quotidien de multiples incidents : en 2009, par exemple, nous avons fait fermer plus de 2 000 sites de phishing. Cela dit, la France n'a connu à ce jour aucune attaque informatique susceptible de paralyser tout un pan de son activité.

Les états et toutes les institutions nationales et internationales sont des cibles pour les pirates informatiques. Il peut s'agir de protestations, cas fréquemment rencontrés, qui se traduisent le plus souvent par l'insertion de revendications sur les sites internet. En France on a ainsi notamment constaté de nombreuses attaques, suite au vote du projet de loi visant à réprimer la contestation de l'existence du génocide arménien, conduites par des pirates revendiquant leur nationalisme turc. Dans un autre registre, on ne compte plus les cas, en particulier dans les pays anglo-saxons, de vol ou de perte de données personnelles dans des systèmes de caisse de retraite, des systèmes fiscaux ou des systèmes médicaux. C'est la confiance du citoyen dans son administration qui est ici en jeu.

On commence aussi à observer des attaques informatiques plus violentes cherchant à paralyser l'activité économique d'un pays, à l'instar des événements qui se sont déroulés en Estonie au mois d'avril 2007 à l'occasion de troubles impliquant la population d'origine russe. Dans ce pays, qui compte parmi les plus connectés du monde, les sites gouvernementaux puis les banques, les médias et les partis politiques furent l'objet d'attaques en saturation qui ont considérablement gêné l'activité du pays. Ces attaques ne furent conduites que par quelques milliers de machines contrôlées à distance par les agresseurs, donc par une force de frappe sans commune mesure avec les capacités des groupes de pirates les plus actifs qui contrôlent des centaines de milliers, voire des millions, d'ordinateurs. Cela nous

laisse entrevoir l'ampleur que prendront les attaques à venir !

Par ailleurs, comme dans le cas des entreprises, les systèmes d'information des institutions deviennent aussi un champ de bataille pour l'espionnage. Les attaques furtives ciblent de plus en plus les états, y compris la France.

La CAIA : votre deuxième priorité est de doter l'État de systèmes sécurisés. Quels sont les systèmes que vous déployez pour les besoins de l'État et des entreprises ?

Patrick Pailloux : Parce que c'est notre mission historique et notre devoir vis-à-vis des acteurs les plus sensibles de l'État tels que les très hautes autorités, les armées, ou la diplomatie, nous devons tout d'abord développer des produits assurant un chiffrement de très haute sécurité, garantissant une protection au niveau secret défense. Développés avec l'aide de la direction générale de l'armement, ces produits (chiffreurs, téléphones...) sont entièrement maîtrisés sur un plan national, depuis le matériel jusqu'au logiciel.

Au-delà des produits, nous assurons la maîtrise d'ouvrage et l'exploitation de réseaux d'état très sécurisés tels qu'ISIS, intranet sécurisé qui permet aux administrations d'interagir en cas de crise et d'échanger de l'information classifiée au niveau "confidentiel défense", et Rimbaud, réseau téléphonique interministériel sécurisé qui relie plusieurs milliers d'autorités à Paris et en régions. Nous fournissons aussi aux hautes autorités des outils sécurisés spécifiques tels que par



Les codes mobiles tu désactiveras

Installés sur les navigateurs internet, les composants ActiveX, JavaScript ou autres permettent des fonctionnalités intéressantes mais ils présentent aussi des risques de sécurité pouvant aller jusqu'à la prise de contrôle par un intrus d'une machine vulnérable. Le navigateur doit être de préférence paramétré de manière sécurisée (mode "internet" des paramètres de sécurité sur internet explorer par exemple) ; pour les sites utiles sur lesquels ce paramétrage ne permet pas d'accéder à toutes les fonctionnalités, celui-ci sera au coup par coup remplacé par un paramétrage plus permissif (mode "sites de confiance" sur internet explorer par exemple). L'utilisation d'un utilitaire spécialisé, tel que No-script pour Firefox, permet d'autoriser aisément, site par site, les fonctionnalités évoluées porteuses de risques.

exemple des systèmes de visioconférences classifiés.

Pour ce qui concerne les entreprises et les systèmes informatiques non classifiés, nous ne sommes pas chargés de déployer des produits de sécurité. En revanche, nous avons une mission de conseil aux administrations et aux opérateurs d'importance vitale que nous allons beaucoup développer dans les prochaines années. Nous accordons aux produits de sécurité des labels attestant de leur qualité après évaluation des produits par des laboratoires français que nous agréons. Le référentiel général de sécurité, qui a été préparé par l'ANSSI et vient d'être publié, systématisera le recours par les autorités publiques aux produits de sécurité labellisés.

J'observe d'ailleurs un manque entre les systèmes de très haute sécurité développés sur crédits publics et les systèmes de sécurité grand public que chacun peut acheter ou trouver sur internet. Nous manquons de produits de qualité, rapidement renouvelés, dont la sécurité serait garantie par l'État et qui pourraient être achetés par les administrations, les opérateurs d'importance vitale, les entreprises... pour protéger leurs réseaux internes, leurs informations sensibles ou classifiées au premier niveau (confidentiel défense). Pour de tels produits, nous avons besoin d'initiatives et de produits industriels que nous labellerions. C'est une priorité pour l'agence.

La CAIA : votre troisième priorité porte sur la sécurité des réseaux de communications électroniques liés aux infrastructures

critiques du pays, notamment celles des opérateurs d'importance vitale. Que doit-on craindre en ce domaine ?

Patrick Pailloux : J'observe que deux grandes tendances se conjuguent : d'une part la technologie internet devient dominante et s'impose partout alors qu'elle est intrinsèquement non sécurisée ; d'autre part l'interconnexion de tous les réseaux se généralise, soit pour des raisons d'économie, soit en raison des exigences de pilotage des entreprises qui nécessitent un accès centralisé à toutes les données, y compris celles liées à la production. De ce fait, les attaques que l'on connaît sur l'internet atteignent désormais l'informatique industrielle, y compris pour des systèmes critiques tels que ceux des opérateurs d'importance vitale. On l'a bien vu l'an dernier avec la propagation du ver Conficker qui a touché des systèmes qu'on aurait pu croire peu vulnérables tels que des appareillages d'hôpitaux ou des systèmes de logistique. Pour l'avenir, nous ne nous faisons pas d'illusion : la menace ne va faire qu'empirer. Aujourd'hui tout est informatisé et nos infrastructures dépendent de plus en plus des systèmes d'information : administrations, hôpitaux, transports, télécoms, énergie, banques... Plus notre société évolue, plus ces systèmes sont interconnectés et proches de l'Internet. Les dysfonctionnements de ces systèmes critiques dont on a besoin pour vivre au quotidien auront des conséquences de plus en plus graves. Comment bien protéger ces infrastructures critiques ? C'est tout l'enjeu des années à venir.

La CAIA : vous évoquez la résilience de l'Internet. Qu'entendez-vous par là ?

Patrick Pailloux : L'accent a été porté pendant la dernière décennie sur le développement des réseaux de communications électroniques, fixes et mobiles, et l'augmentation de l'offre par la concurrence. Ces efforts ont conduit à de grandes réussites dont nous bénéficions tous les jours. Mais la sécurité n'a pas été considérée comme prioritaire pendant cette période, ce qui fait que les réseaux sont fragiles alors qu'ils forment, de plus en plus, les systèmes nerveux de notre société. Tout reste donc à faire en la matière, sur le plan national comme sur le plan européen d'ailleurs : je pense en particulier à la sécurisation des infrastructures physique (nœuds d'interconnexion...) ou logique (système des serveurs de noms de domaine - DNS, qui est à la base du fonctionnement de l'internet). Il nous faut également fixer des règles de sécurité uniformes pour les opérateurs, qui ne limiteront pas la concurrence mais élèveront le niveau de sécurité de tous les opérateurs.

La CAIA : on sait que la sécurité informatique est un sujet complexe, dans lequel les attaquants vont souvent plus vite que les défenseurs. Vous avez les moyens de cette politique ?

Patrick Pailloux : C'est sur la base du constat que vous faites que les autorités françaises ont décidé de créer l'agence et d'en doubler les effectifs pour les porter à 250 personnes.



Compte tenu du turn-over important dans ce métier, je recrute près de 70 personnes chaque année, ce qui est très ambitieux pour une agence qui compte aujourd'hui 130 personnes !

La CAIA : vous communiquez sur tous ces sujets ?

Patrick Pailloux : Oui, et il faut bien reconnaître que c'est assez nouveau dans ce domaine qui a longtemps été recouvert d'un voile de secret. Nous avons naturellement un site internet sur lequel de nombreux conseils et informations peuvent être trouvés. Nous avons aussi créé un site grand public, www.securite-informatique.gouv.fr, qui a vocation à aider tout un chacun à se prémunir des principaux risques informatiques et relaye toutes sortes d'informations pratiques et d'actualités sur le sujet. Nous avons édité le Passeport de conseils aux voyageurs, un petit guide des précautions à prendre lorsqu'on se déplace à l'étranger avec son ordinateur ou son téléphone portable, qui est joint au présent numéro du magazine de la CAIA.

La très haute sécurité au profit des fonctions régaliennes de l'État reste une priorité pour nous, naturellement. Mais nous ne pouvons nous en tenir à cette extrémité du spectre. La sécurité nationale suppose aussi la protection des systèmes informatiques des administrations, des opérateurs d'importance vitale et de nombreux autres acteurs, entreprises ou centres de recherche. Le facteur humain est souvent le point faible

de la sécurité d'un système d'information, il nous faut donc sensibiliser le plus large public possible sur ces sujets. Je constate que les bonnes pratiques élémentaires de sécurité dans l'utilisation de l'informatique ne sont pas encore vraiment entrées dans les mœurs en France. Les particuliers n'ont pas encore intégré les réflexes sécuritaires de base. Quant aux entreprises, elles accusent souvent un certain retard et ont tendance à cacher les incidents qui les affectent. Nous sommes loin derrière les Anglo-saxons en matière de sécurité et de transparence. Pour que les mentalités évoluent, il est essentiel que les Français soient bien informés et prennent toute la mesure du problème.

La CAIA : et vos sites n'ont jamais été attaqués ?

Patrick Pailloux : Si bien sûr, ils le sont régulièrement. Mais à ce jour, personne n'a encore réussi à s'y introduire !

La CAIA : le Livre blanc annonce la création d'une capacité d'attaque informatique française. Que pouvez-vous nous dire à ce sujet ?

Patrick Pailloux : La mission de l'agence porte sur la prévention des attaques et la défense face aux agressions informatiques, et c'est déjà énorme. Elle ne s'étend ni aux actions offensives sur les réseaux, ni d'ailleurs aux missions de police, de justice ou de renseignement. Étant chargé d'une mission exclusivement défensive, je ne peux donc

m'exprimer sur ce sujet qui ne relève pas de mes compétences.

La CAIA : combien d'ingénieurs de l'armement employez-vous ?

Patrick Pailloux : Beaucoup trop peu ! Seuls trois ingénieurs de l'armement font aujourd'hui partie de l'agence, dont deux sont membres du comité de direction et s'expriment d'ailleurs dans ce numéro de la revue. Je regrette qu'aucune arrivée d'IA n'ait eu lieu depuis 5 ans malgré mes sollicitations. Je pense qu'un service interministériel, relevant du secrétariat général de la défense et de la sécurité nationale, à vocation technique, en relation quotidienne avec la défense et la DGA, devrait intéresser davantage les ingénieurs de l'armement.

La mission qui nous est confiée est celle de défendre notre pays contre une nouvelle sorte de menace. Il y a dans ce domaine tout à faire, tout à inventer. C'est une aventure motivante !

La CAIA : Patrick Pailloux, la CAIA vous remercie pour vos propos et, surtout, vous souhaite un plein succès dans votre mission !

Propos recueillis par
Yves Le Floch

**Whatever the mission,
wherever, whenever**

SHERPA LIGHT

The world over, vehicles from Renault Trucks Defense offer the best protected land force mobility.

www.renault-trucks-defense.com



**RENAULT
TRUCKS**

Defense



Sécurité et confiance numériques

Les nouveaux enjeux de la sécurisation numérique dans les Armées



par **Marc Sirven**

Ingénieur en chef de l'armement

En poste successivement au Centre d'électronique de l'armement puis à la Direction Centrale de la Sécurité des systèmes d'information (99-05), Marc Sirven est actuellement en charge de la préparation des futurs programmes du système de force Commandement et Maîtrise de l'information à la DGA

Comme le souligne le Livre blanc sur la défense et la sécurité nationale, les moyens d'information et de communication sont devenus le système nerveux de nos sociétés, sans lequel elles ne peuvent plus fonctionner. Leur sécurisation est devenue un enjeu majeur. L'émergence de cette société de l'information touche également profondément les forces armées. On se propose dans cet article de présenter quelques-uns des nouveaux enjeux de la sécurisation numérique dans les systèmes des Armées.

Omniprésence des technologies civiles

Les nouvelles technologies de l'information du monde civil innervent de plus en plus rapidement et de plus en plus profondément les systèmes des Armées. La numérisation du champ de bataille ne relève plus du simple concept mais devient chaque jour de plus en plus une réalité : dans les postes de commandement, les ordinateurs et les écrans géants remplacent les cartes murales ; en opération, les outils de "chat" sont utilisés pour l'échange d'informations en temps réel ; le contrôleur aérien n'a plus à guider le pilote de chasse qui dispose, via sa liaison de données, de toute la situation tactique.

Cette invasion des systèmes d'information touche également directement les systèmes

d'arme. D'ici peu, le chef d'unité ayant identifié son objectif dans ses jumelles n'aura qu'à cliquer sur un bouton pour que la tourelle du char voisin s'oriente automatiquement pour engager la cible. La numérisation du champ de bataille va modifier sensiblement la manière de conduire des opérations militaires. Autrefois cantonnées à quelques spécialistes des transmissions, les problématiques de sécurisation de l'information sont maintenant généralisées et sources de nouveaux enjeux.

Les attaques informatiques majeures

Premier enjeu, la nouvelle menace que constituent les attaques informatiques. Basées sur les technologies de l'Internet, les systèmes des Armées sont potentiellement

tout aussi vulnérables que les systèmes civils à ces attaques informatiques. Être à même de résister aux attaques informatiques nous oblige à revoir profondément notre approche de la sécurité : marquée par la Seconde Guerre mondiale, où les alliés décryptaient les communications stratégiques allemandes, la sécurisation de nos systèmes d'information a été surtout axée sur la protection des communications contre les interceptions via le chiffrement.

Cette défense statique (statique parce qu'une fois qu'on avait mis des chiffreurs, le travail était fini) n'est pas suffisante face aux nouvelles menaces qui exploitent toutes les vulnérabilités des logiciels : il est nécessaire d'adopter une approche beaucoup plus dynamique incluant une capacité de détecter



Avec prudence tu cliqueras

Un grand nombre d'attaques informatiques se présentent sous la forme de messages trompeurs malveillants, accompagnés de pièces jointes ou de liens à cliquer. Les plus sophistiquées d'entre elles peuvent sembler provenir d'une personne connue, voire paraître identiques à un message déjà reçu. L'ouverture de la pièce jointe ou le clic sur le lien peuvent entraîner la prise de contrôle de la machine par l'attaquant, à l'insu de l'utilisateur. Autre risque très fréquent, celui de messages semblant provenir d'organismes honorables et incitant, via une page semblant légitime, à dévoiler ses identifiants personnels. Parmi les précautions utiles, il vaut mieux saisir soi-même l'adresse du site dans la barre d'adresse du navigateur plutôt que de cliquer un lien peu sûr.

une attaque informatique et de réagir. C'est ce qui a conduit le Gouvernement à constituer un centre de "détection précoce".

"La numérisation du champ de bataille va modifier sensiblement la manière de conduire des opérations militaires"

Des premières actions sont en cours pour développer de telles capacités sur les réseaux militaires d'infrastructures, qu'il faudra généraliser à l'ensemble des systèmes d'information même dans les niveaux très tactiques. Cette approche de la sécurisation fondée sur la détection et la réaction est encore jeune. Les exemples quotidiens de vol de données bancaires, de piratage de serveurs... nous montrent qu'il y a encore beaucoup à faire pour que la défense puisse prendre le pas sur l'attaque. Il y a donc là un domaine de recherche particulièrement stimulant, surtout dans le contexte militaire : comment détecter et reconnaître une attaque ? Comment réagir ?

Nouvelles technologies et réglementation

En plus de détecter une attaque, il faut essayer de sécuriser au mieux tous les

nouveaux systèmes d'information avant leur utilisation opérationnelle pour les rendre les moins vulnérables possibles. Cette sécurisation est loin d'être évidente tant il est aujourd'hui plus aisé de trouver une vulnérabilité dans un logiciel que d'en produire un sans faiblesse. Elle est aussi rendue difficile parce que la réglementation en matière de SSI, encore très largement héritée de la guerre froide, est peu adaptée au rythme d'évolution des nouvelles technologies.

Les règles de l'OTAN imposent par exemple qu'une information NATO Secret soit protégée par un chiffreur "hardware" (pas question d'utiliser un logiciel) qui aura été préalablement évalué par l'agence SECAN hébergée aux États-Unis. Réaliser un chiffreur qui respecte ces règles demande des années. A moins d'avoir su brillamment anticiper les besoins futurs, il est extrêmement difficile de répondre aux urgences opérationnelles en respectant ces règles. Il ne faut donc pas trop s'étonner que les images de certains drones en Afghanistan soient interceptées par les Talibans. L'urgence opérationnelle a primé.

Nos réglementations en matière de sécurité sont encore très exigeantes. Faire évoluer la réglementation dans le sens d'un plus grand pragmatisme et d'une gestion du risque plus flexible serait très profitable.

Les conséquences du retour dans l'OTAN

Dernier enjeu, qui n'est pas lié aux nouvelles technologies, les conséquences de la pleine

participation de la France à l'OTAN. Celle-ci va nous conduire à basculer une grande partie de nos systèmes d'information du monde du classifié Défense français au monde du classifié OTAN. Il va certes rester des réseaux dits de souveraineté, "spécial France", dans le renseignement ou le nucléaire par exemple, mais ils ne représenteront qu'une petite partie de nos systèmes et non plus la grande majorité comme jusqu'alors. C'est dans le développement des produits de sécurité que cette bascule dans le monde OTAN va être marquante. Dans un contexte budgétaire très contraint, l'enjeu va consister à maintenir notre capacité à maîtriser en France ces technologies de souveraineté que sont les produits cryptographiques alors que l'essentiel de nos besoins portera sur des produits approuvés par l'OTAN. Être capable de développer des gammes de produits permettant pour un surcoût marginal de répondre à la fois à nos besoins "FR eyes only" et OTAN est un véritable défi pour les années à venir.

L'arrivée des nouvelles technologies de l'information et de la communication dans les Armées a de profondes implications. Même si les Armées sont depuis longtemps sensibilisées à la protection de l'information, celle-ci oblige à reconsidérer notablement la façon d'appréhender la sécurité de nos systèmes d'information et de communications. Que tous ceux que le sujet intéresse se réjouissent, il y a encore beaucoup de choses à faire dans ce domaine dont tout le monde s'accorde à dire qu'il doit être renforcé. ☞

Sécurité et confiance numériques

Cryptologie et recherche académique



par **Antoine Joux**

Ingénieur en chef de l'armement

DGA/DS/MRIS, Mission pour la recherche et l'innovation scientifique, Professeur associé à l'université de Versailles Saint-Quentin-en-Yvelines

Face au rapide développement des technologies numériques, la cryptologie doit offrir de nouvelles solutions pour répondre à cette nouvelle demande.

Comment la recherche académique, en particulier en France, contribue-t-elle à ces progrès ?

Depuis l'invention de la cryptographie à clef publique par Diffie et Hellman en 1976, la cryptologie est devenue une discipline de recherche académique, touchant à la fois aux mathématiques et à l'informatique. En pratique, les algorithmes et protocoles cryptographiques sont essentiels pour assurer la sécurité de tout système d'information. Cependant, cette mise en œuvre n'est pas simple. En effet, il importe, d'un côté, d'utiliser des méthodes éprouvées, car l'expérience montre que l'improvisation d'algorithmes ou de protocoles conduit toujours à la catastrophe. Mais, d'un autre côté, il ne faut pas considérer la cryptographie comme une discipline morte n'ayant pour but que de consolider les acquis des années 70. Bien au contraire, les progrès récents de la recherche académique ouvrent la voie pour de nouvelles applications.

Quelques avancées récentes

Pour illustrer cette tendance, prenons quelques exemples, sans doute arbitraires, de telles avancées. Pour commencer, intéressons-nous aux progrès importants de la cryptanalyse des fonctions de hachage, intervenus depuis 2004. Pour mémoire, les fonctions de hachage sont, avec le

chiffrement, l'une des briques fondamentales de la cryptographie moderne. Ces fonctions permettent de transformer un document quelconque en une empreinte courte pouvant servir d'identifiant unique du document. Cette fonctionnalité est par exemple indispensable dans les applications de signatures numériques. Mais les fonctions de hachage ont bien d'autres utilisations. Trop, diront certains. En effet, elles peuvent servir à générer des nombres pseudo aléatoires, à augmenter le niveau de sécurité de systèmes de chiffrement à clef publique... En contrepartie, ces fonctions doivent répondre à de nombreuses exigences de sécurité. Elles doivent être à sens unique, sans préimage, sans collision... Pour répondre à cette demande, l'industrie disposait en 2000, de plusieurs fonctions standardisées. Certaines étaient mal dimensionnées, avec une sortie sur 128 bits seulement, mais d'autres comme la fonction SHA-1 (standardisées par le NIST) semblaient parfaitement adaptées. Malheureusement, suite au perfectionnement des méthodes de cryptanalyse, ces fonctions se sont avérées moins sûres qu'elles ne le semblaient. Aujourd'hui, dans le cadre d'un appel lancé par le NIST, une grande partie de la communauté est mobilisée pour

construire un nouveau standard capable de répondre à l'ensemble des exigences.

Prenons comme deuxième exemple la naissance, en 2000, d'une nouvelle branche de la cryptographie : la cryptographie basée sur les couplages. C'est une extension de la cryptographie basée sur les courbes elliptiques, qui se fonde sur la possibilité sur certaines courbes elliptiques de calculer à partir de 2 points de la courbe un nombre (dans un corps fini), avec la propriété importante que ce couplage est bilinéaire. Ainsi, si l'un des points est multiplié par a et l'autre par b , alors le résultat du calcul est élevé à la puissance ab . Cette propriété d'apparence anodine, avait déjà permis dans les années 90 de montrer que certaines courbes elliptiques offrent une sécurité moins importante que d'autres. La cryptographie basée sur les couplages permet de généraliser l'échange de clef de Diffie et Hellman pour partager un secret entre 3 personnes au lieu de 2. Elle permet aussi de résoudre un problème ouvert posé par Shamir en 1984, celui de la cryptographie basée sur l'identité : comment envoyer un message secret à une personne, si l'on ne partage aucun secret avec elle et si l'on ne connaît rien d'autre que son nom et son adresse ?

Les logiciels incertains tu éviteras

Qu'il s'agisse de logiciels entiers ou de greffons sur des logiciels de base ("plug-ins" en anglais), il convient de s'assurer que le logiciel provient d'une source honorable et de n'installer que des logiciels dont on a réellement besoin.



Sécurité : le défi des nouvelles technologies numériques

Les nouveaux téléphones portables avec leurs fonctionnalités irremplaçables ; les automobiles intelligentes capables de prévoir et d'éviter les embouteillages, de limiter leur consommation d'énergie, d'assister les manœuvres complexes grâce à un ordinateur de bord connecté en temps réel ; les puces sans contact permettant de réaliser des inventaires permanents sans difficultés, de payer instantanément au supermarché sans vider son chariot. Toutes ces technologies promettent de nous faciliter la vie quotidienne et présentent des avantages indéniables. Bien sûr, comme toute évolution de grande ampleur, elles ont des conséquences sur la société, mais leurs défenseurs estiment qu'à terme leurs bénéfiques compenseront largement leurs inconvénients.

En revanche, un effet secondaire important de ces technologies est souvent sous-estimé : leur impact en termes de sécurité. Pirater un téléphone suffit à obtenir de nombreuses informations personnelles sur son détenteur. Prendre le contrôle à distance d'un véhicule trop sophistiqué permet d'imaginer le crime parfait. Neutraliser une puce sans contact peut devenir le nouveau credo des voleurs à l'étalage. Bricoler des machines à voter peut permettre un coup d'état discret et pacifique. Enfin, le risque d'une surveillance de tous les instants portant atteinte à la vie privée n'est pas à négliger.

Pour lutter contre toutes ces dérives, le défi consiste à mettre en place des mesures de protection, efficaces techniquement et compréhensibles par le plus grand nombre. En effet, en l'absence d'une bonne compréhension des risques, l'utilisateur final peut souvent être amené par tromperie à porter atteinte à sa propre sécurité, par ce que l'on appelle souvent l'ingénierie sociale.

Pour des applications s'appuyant sur une autorité centrale de confiance, la cryptographie basée sur l'identité est une alternative commode capable de se substituer à la mise en place, toujours lourde et coûteuse, d'annuaires de clefs publiques. Depuis 2000, des centaines d'articles de recherche utilisent les couplages et en proposent une multitude d'applications.

Bien sûr, comme dans tous les domaines de recherche, toutes les avancées ne font pas l'unanimité. Ainsi, ce que l'on appelle la sécurité prouvable des protocoles cryptographiques fait aujourd'hui débat. Historiquement, un système cryptographique était présumé sûr, jusqu'à ce qu'une nouvelle technique de cryptanalyse lui donne le coup de grâce. Avec l'apparition de la cryptographie académique, la question de donner une garantie de sécurité est apparue. Ainsi, on dit souvent que la sécurité du système RSA repose sur la difficulté de factoriser des grands nombres. Mais, une telle assertion est à la fois inexacte et imprécise. Qu'appelle-t-on sécurité ? Quels sont les nombres difficiles à factoriser ? Est-ce vraiment le bon problème difficile à considérer ?

C'est toute la difficulté de la sécurité prouvable

dite réductionniste. On va pouvoir démontrer que dans un modèle d'attaque précis, un attaquant capable de mettre à mal la sécurité d'un système cryptographique donné pourra résoudre un problème mathématique ou algorithmique réputé difficile. Mais, le diable est comme toujours dans les détails et de nombreux systèmes "prouvés sûrs" se sont retrouvés attaqués. Parfois la preuve était fautive, mais le plus souvent, c'est le modèle d'attaquant qui est trop restrictif ou le problème sous-jacent qui devient facile pour les tailles de clefs choisies. Il importe donc d'être prudent, sans pourtant tout jeter aux orties, comme certains voudraient le faire un

peu vite. Enfin, il ne faut pas oublier que la cryptographie seule ne suffit pas à assurer la sécurité des systèmes. Il importe également de prendre en compte sa mise en œuvre et son environnement. Ainsi, l'étude de la sécurité de cette mise en œuvre, plus particulièrement dans du matériel dédié, est essentielle. Depuis une dizaine d'années, une conférence spécifique est d'ailleurs consacrée à cette thématique. A titre d'exemple, l'étude de la sécurité du chiffrement sur processeur généraliste a conduit Intel à introduire dans ses nouveaux processeurs des instructions spécifiques dédiées au chiffrement AES. 🐼

La recherche académique en France

Historiquement, la France fait partie des nations qui ont contribué au développement de la cryptographie. Il n'est donc pas surprenant qu'une large communauté académique, dont le principal fondateur reconnu est Jacques Stern, s'y soit développée. Ainsi le CNRS recense une vingtaine de laboratoires en mathématique et en informatique s'intéressant à cette thématique. En ne comptant que les membres de l'IACR (association internationale de recherche en cryptographie), la population des chercheurs français en cryptographie est de 120 sur un effectif mondial d'environ 1500. De plus, parmi les treize membres élus du comité directeur de cette association, on ne compte pas moins de quatre français (et descendants scientifiques de Jacques Stern).

Sécurité et confiance numériques

Les dimensions géopolitiques de la sécurité numérique

De la sécurité numérique à la guerre numérique



par **Alain Esterle**

Chercheur associé de la Fondation pour la Recherche Stratégique
Consultant indépendant

X67, PhD Mathématiques Appliquées, diplômé en Études Politiques, directeur adjoint de la DCSSI de 2000 à 2005, puis Chef du département technique d'ENISA jusqu'à l'été 2008. Aujourd'hui, chercheur associé de la Fondation pour la Recherche Stratégique et consultant indépendant spécialisé en sécurité des systèmes d'information et en protection des données personnelles.

La sécurité numérique est devenue un élément majeur de la géostratégie internationale, à la fois outil de confrontation et thème de coopération. Sommes-nous pour autant à la veille ou à l'heure de la guerre numérique ? Un état des lieux s'impose.

Le Livre blanc sur la défense et la sécurité nationale a jugé les attaques informatiques plus menaçantes que les attaques balistiques (mais moins que le terrorisme), et a préconisé le développement national d'une capacité de lutte informatique offensive. Le Royaume Uni a créé un Bureau de cyber-sécurité au sein du Cabinet Office et un Centre opérationnel en cyber-sécurité implanté au GCHQ, tout en laissant entendre sa vocation à disposer d'une capacité offensive. Le président Obama a nommé Howard Schmidt comme

coordinateur national en cyber-sécurité, dans le sillage de la Cyberspace Policy Review et de l'Initiative nationale en cyber-sécurité globale.

Beaucoup de pays se préparent aujourd'hui, ouvertement ou non, à la guerre numérique. Mais contre quels adversaires, pour quels enjeux, au sein de quelles coalitions ?

Enjeu majeur dans les relations entre les États, la maîtrise de l'information l'est plus que jamais à l'heure du cyberspace,

comme est venue le rappeler l'affaire Échelon. L'américain Joseph Nye, adepte du soft power, prophétisait à la fin des années 90 que la domination en matière d'information permettrait, comme en matière nucléaire, de dissuader l'adversaire d'agir tout en contrôlant l'allié placé en situation de dépendance : l'information dominante allait devenir l'axe majeur de la géostratégie. Mais c'était avant le 11 septembre 2001. Qu'en est-il en 2010 ?

Les avertissements de sécurité jamais tu n'ignoreras

Doivent en particulier alerter les avertissements liés à l'installation d'un logiciel, dont il faut s'assurer de la provenance, ou liés aux certificats de sécurité utilisés par les sites internet sécurisés (par défaut, un avertissement signalant un certificat non reconnu ou auto-signé doit être considéré comme une présomption d'interception de la communication avec le site sécurisé).



Approches européennes en matière de sécurité numérique :

- L'Agence Européenne en Sécurité des Systèmes d'Information (ENISA), créée en 2004, répond au besoin de sécurité et de confiance indispensable au développement de la société de l'information (stratégie de Lisbonne). Ses missions devraient inclure prochainement des fonctions opérationnelles (protection des institutions européennes).
- L'Europe de la défense et les relations avec l'OTAN ont conduit le Conseil européen à sécuriser les informations classifiées, y compris sous forme numérisée.
- Les recherches en sécurité globale, notamment pour la protection des infrastructures, sont devenu un thème à part entière du programme cadre de R&D.

La sécurité numérique au cœur de confrontations internationales variées

L'attaque par déni de service qui a frappé l'Estonie au printemps 2007 était peu coordonnée au début, beaucoup mieux dans sa seconde phase. Elle démontre qu'il était possible de paralyser des secteurs entiers d'un pays pendant plusieurs semaines. Elle a aussi poussé l'Europe et l'OTAN à développer des capacités de cyberdéfense, même si l'implantation à Tallin d'un centre d'excellence avait été décidée auparavant.

La campagne militaire de la Russie contre la Géorgie en 2008 a été accompagnée d'une attaque en déni de service des sites gouvernementaux et des médias. La phasage étroit avec les actions militaires, ainsi que la rapidité d'enregistrement de nouveaux noms de domaine et de création de sites web, suggèrent que l'ensemble était préparé d'avance, même si rien ne démontre que les services gouvernementaux russes ont été directement impliqués dans la phase d'exécution.

En juillet 2009, trois vagues d'attaques informatiques ont frappé les sites sud-

coréens de banques, du Parlement, des ministères des affaires étrangères et de la défense, dans un contexte de tension accrue avec la Corée du Nord.

Plus récemment, l'adoption en mars 2010 par le Parlement suédois d'une résolution condamnant le génocide arménien a été suivie d'une série d'attaques informatiques contre les sites d'institutions publiques suédoises.

Dans certains pays, la sécurité de l'information s'entend aussi, voire d'abord, comme le contrôle du contenu et de l'accès des internautes à certaines informations. La censure imposée par la Chine à l'usage du moteur de recherche Google et le refus de Google de s'y plier montrent comment la nature même d'Internet peut exacerber des différences de conception sur les droits individuels.

Des confrontations existent aussi entre pays "occidentaux". La protection des données personnelles est un droit fondamental en Europe, indissociable des questions de sécurité de l'information, alors que son approche est beaucoup plus souple aux États-Unis. Alors que la gestion des données personnelles par ce même

Google ne pose pas de problème au-delà de l'Atlantique, elle a donné lieu à une audition devant le Parlement européen. Ce dernier est aujourd'hui très réticent à l'adoption d'un accord permettant au Trésor et aux agences américaines d'accéder, au nom de la lutte anti-terroriste, aux données bancaires des citoyens européens émetteurs ou bénéficiaires d'une transaction (données SWIFT). Dans le cas des entreprises, peut s'y ajouter la suspicion d'espionnage économique.

La sécurité numérique, moteur de coopérations

Dès novembre 2001, le conseil de l'Europe a adopté une convention internationale sur la cybercriminalité, fondant des concepts communs non seulement en matière d'infractions et de prévention des fraudes, mais aussi en matière de coopération et d'entraide entre les pays signataires.

La protection des infrastructures vitales (critiques selon la terminologie américaine ou essentielles selon la canadienne) est devenue un enjeu commun et un axe fort de coopération entre états à la suite des attentats sur New-York, Londres et Madrid.



La menace chinoise

La Chine a adopté une stratégie à très long terme d'investissement massif sur les technologies de l'information et de la communication afin de contrer la supériorité américaine dans le domaine des technologies de défense. L'omniprésence sur le net de ses hackers, dont des publications académiques évaluent le nombre à plusieurs dizaines de milliers, encadrés ou non par le gouvernement, témoigne de cette ambition. Cet effort intensif, très organisé et systématique de piratage permet aux services chinois de récupérer d'énormes quantités de données sensibles ou classifiées concernant les opposants au régime, les entreprises technologiques occidentales, les forces armées concurrentes...

Outre l'art du piratage informatique, la Chine développe de manière extrêmement résolue de grands groupes industriels nationaux qui exportent partout dans le monde une technologie "made in China". Ainsi, la société chinoise Lenovo, créée il y a vingt ans, a acquis en 2005 la totalité de la division PC d'IBM et vend maintenant pour environ 15 Md\$ d'ordinateurs par an, pour moitié en-dehors de Chine, ce qui en fait le quatrième fabricant mondial. Dans le domaine des équipements de communications électroniques, les sociétés Huawei et ZTE, créées dans les années 1980 à partir des compétences d'état, se sont hissées au quatrième et neuvième rang mondial et font désormais de l'ombre à Alcatel-Lucent, Ericsson et Nokia-Siemens. En 2008, leur chiffre d'affaires combiné dépassait déjà celui du numéro 1 mondial et leur progression se poursuit avec la même dynamique.

La très grande proximité entre ces industriels et l'administration chinoise fait craindre à certains gouvernements occidentaux que le déploiement d'équipements chinois dans les réseaux des opérateurs de communications électroniques soit porteur de grandes vulnérabilités. Les équipements de télécom sont par nature fortement connectés aux réseaux extérieurs et, comme la plupart des machines informatiques, présentent de nombreuses failles et vulnérabilités ; un constructeur intrusif peut aisément se servir de celles-ci comme des "back-doors", ou pièges informatiques, et les exploiter à distance afin de capter les communications sensibles ou d'entraver fortement le fonctionnement des réseaux en cas de crise.

Les 10 principes adoptés par le G8 en 2003 ont été relayés par l'OCDE en 2008, mais surtout l'Europe a bâti progressivement une politique cohérente combinant responsabilité nationale pour protéger les infrastructures à caractère strictement national et responsabilité européenne dès que la défaillance d'une infrastructure affecterait plusieurs pays européens. Échanges d'information et de bonnes pratiques, programmes spécifiques de recherche, exercices paneuropéens sont les éléments clés de cette démarche rattachée au cadre général de "la prévention, la préparation et la gestion des conséquences en matière de terrorisme et autres risques liés à la sécurité". La résilience des infrastructures critiques d'information (réseaux publics et SCADA) y tient une place importante, y compris dans les travaux d'ENISA (voir encadré).

Reste qu'Internet, dont le protocole devient

la norme pour tout échange d'information électronique, est intrinsèquement non sécurisé (n'ayant pas été bâti pour ça) et que sa gestion reste très largement pilotée par les instances américaines, notamment à travers un Memorandum of Understanding passé entre le gouvernement américain et l'ICANN, instance de gestion des noms de domaines et adresses IP. Le devenir d'Internet et de sa gestion est un sujet de débat continu, notamment dans le cadre onusien de l'Internet Governance Forum : certainement une négociation qui a de beaux jours devant elle.

Point final dans ce panorama des dimensions géopolitiques de la sécurité numérique, le débat au sein de l'ONU concernant l'adoption d'un traité sur la guerre informatique. Non pas que ce débat doive changer l'évolution des choses mais parce qu'il est révélateur des oppositions

politiques et des rapports de force actuels. Deux thèses en présence : les États-Unis préconisent un renforcement des coopérations dans la lutte contre la cybercriminalité, au motif que cela devrait développer la sécurité dans le cyberspace, y compris en cas d'action militaire.

De son côté, la Russie milite pour un traité de désarmement analogue à celui sur les armes chimiques, dans le but avoué d'éviter une nouvelle course aux armements.

Mais trop de pays sont déjà engagés dans la lutte informatique défensive et (plus ou moins ouvertement) offensive pour que l'on puisse encore douter qu'elle a déjà commencé. ☞

'Supervisory Control And Data Acquisition : concerne les réseaux opérationnels spécifiques des entreprises

Sécurité et confiance numériques

La guerre des mondes numériques aura bien lieu

Du mythe à la réalité



par **Florent Chabaud**

Ingénieur en chef de l'armement

Sous-directeur assistance, conseil et expertise de l'ANSSI

X89-ENSTA94, docteur en informatique, cryptologue puis coordinateur de la sécurité du système de messagerie MUSE au CELAR de 1996 à 2000, chef du laboratoire des technologies de l'information puis sous-directeur scientifique et technique de la DCSSI jusqu'en 2009.

En 1983, en pleine guerre froide, le film "WarGames" est un succès cinématographique qui ancre l'image ludique du jeune hacker dont les actions insouciantes n'ont de conséquences graves que parce qu'elles s'appliquent par inadvertance à un système militaire contrôlant l'arsenal nucléaire des États-Unis. Trente ans plus tard, la guerre froide n'est plus, mais celle du cyberspace a déjà commencé et ce n'est pas un terrain de jeux d'adolescents !

Le monde numérique fascine par son caractère virtuel et échappe à la compréhension par sa complexité. Énumérer la liste des menaces pourtant avérées qui pèsent sur lui vous fait passer pour un paranoïaque réfractaire au progrès. Ajoutez-y une analyse d'impact de ces menaces sur le monde réel et on vous complétera le diagnostic précédent de l'adjectif "incurable" ! Et pourtant, un décideur responsable doit prendre en compte ce risque.

Car la menace informatique est tout sauf virtuelle. Tout ce que vous pourriez en imaginer s'est déjà concrétisé dans des scénarios dignes de la science-fiction. Ainsi, début 2009, la presse titrait : "le Rafale cloué au sol par le virus Conficker". S'il faut faire la part des choses entre exagération médiatique et réalité des faits (les avions n'ont pas été infectés et la décision de surseoir aux vols relevait d'un principe de précaution), force est de constater qu'un

virus informatique peut effectivement avoir un impact, même sur des systèmes d'information militaires, qu'on imagine parmi les mieux protégés.

Des millions de machines sous contrôle

Le mythe de l'adolescent boutonneux doit laisser place à la réalité d'attaques ciblées, organisées, financées pour un objectif quantifié. Considérons par exemple le Mariposa Botnet, un réseau de machines zombies¹ estimé à 12 millions d'ordinateurs infectés, répartis dans 190 pays, dont les trois personnes soupçonnées de le contrôler ont été arrêtées courant février en Espagne. Le contrôle de ce type de réseau offre des sources de financement importantes, par la simple location sur le marché parallèle de l'énorme capacité informatique qu'il représente. Songez qu'en 2007, pour gravement perturber pendant plusieurs jours

les infrastructures numériques de l'Estonie, environ 2000 machines avaient suffi. Pas étonnant que les vulnérabilités des systèmes d'exploitation, qui permettent de prendre le contrôle des ordinateurs, s'échangent à prix d'or et alimentent un marché noir que les conférences de hackers tentent de concurrencer².

Mais le professionnalisme des attaquants va plus loin. Fin 2008, on annonçait que plusieurs centaines de terminaux de paiement avaient été piégés par une organisation criminelle avant même leur livraison³, en ajoutant des composants afin de récolter informations bancaires et codes secrets des clients. Réaliser et rentabiliser une telle opération nécessite d'être bien organisé.

La défense doit se hisser au niveau de l'attaque

Bien évidemment, si des organisations

Sécurité et confiance numériques

Le référentiel général de sécurité (RGS)

Pour l'administration française, les responsabilités en matière de sécurité des systèmes d'information sont désormais réglementées : "l'autorité administrative doit, afin de protéger un système d'information :

1° Identifier l'ensemble des risques pesant sur la sécurité du système et des informations qu'il traite (...);

2° Fixer les objectifs de sécurité (...) pour répondre de manière proportionnée au besoin de protection du système et des informations face aux risques identifiés ;

3° En déduire les fonctions de sécurité (...) qui permettent d'atteindre ces objectifs et respecter les règles correspondantes du référentiel général de sécurité.

Dans les conditions fixées par le référentiel susmentionné, l'autorité administrative réexamine régulièrement la sécurité du système et des informations en fonction de l'évolution des risques.

L'autorité administrative atteste formellement auprès des utilisateurs de son système d'information que celui-ci est protégé conformément aux objectifs de sécurité fixés (...)."

Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

criminelles sont à même de monter des opérations d'envergure, il en va de même des services spécialisés de renseignement, publics comme privés, et la France n'est pas à l'abri (voir illustration). Toute grande entreprise a déjà été confrontée à des actions malveillantes d'intelligence économique utilisant des attaques informatiques. La récente intrusion sur les systèmes de Google, attribuée à la Chine, a ainsi occasionné un regain de tension dans les relations diplomatiques sino-américaines⁴. Mais si l'avantage est pour le moment à l'attaque, la défense informatique a des arguments à faire valoir.

Le monde numérique, pour être virtuel, dispose d'outils pour renforcer sa défense. La cryptographie offre des mécanismes solides, résistants à toute attaque connue, qui sont déjà employés. Reste que la cryptographie ne fait pas tout : encore faut-il qu'elle ne soit pas contournée trivialement par floutage⁵. Ce ne sont donc pas tant les technologies qui manquent, que la prise en compte systématique de la sécurité des systèmes d'information (voir encadré). L'amateurisme dans ce domaine est suicidaire. Notre société doit organiser sa défense informatique avec

la même détermination que les attaquants auxquels elle est confrontée.

Authenticité et disponibilité sont les deux piliers de la confiance numérique

La sécurité informatique est souvent associée à la confidentialité et à la cryptographie. Mais nos systèmes d'information sont désormais critiques pour notre société et doivent avant tout être disponibles. Ceci passe par une maîtrise plus grande de leurs constituants. Les dernières études montrent en effet que des équipements comme les cartes réseaux, qui coûtent quelques euros, sont loin d'être anodins pour la sécurité, puisque leur prise de contrôle à distance est envisageable, sans qu'aucun dispositif de sécurité de la machine qui les utilise ne puisse l'empêcher⁶.

La certification des composants utilisés dans nos réseaux par des laboratoires accrédités, la mise en place d'infrastructure de gestion des identités numériques et des clés cryptographiques associées sont autant d'efforts d'organisation à mener pour que la défense reprenne l'avantage. Ceci passe par une mobilisation générale, non seulement des



Un terminal de paiement électronique pour carte bancaire
©Aurélien Haberstich

experts, mais de tous les acteurs responsables. Garantir l'authenticité des matériels, des logiciels et des informations traitées est l'enjeu principal de la confiance numérique. ☞

Les procédures triviales de recouvrement de mot de passe tu fuiras

De nombreux sites et services en ligne proposent, en cas de perte du mot de passe, de répondre à une ou deux questions simples pour le retrouver. Ces mécanismes sont bien souvent sources de compromission totale des comptes personnels, risque majeur notamment dans les messageries. S'ils ne peuvent être désactivés, il convient pour le moins que les réponses à fournir ne soient pas devinables.



Géolocalisation de machines zombies participant à une attaque en déni de service distribué contre une administration française ©Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques (CERTA)

¹Un Botnet est un réseau de machines compromises à la disposition d'un individu malveillant (le maître). Ce réseau est structuré de façon à permettre à son propriétaire de transmettre des ordres à tout ou partie des machines du botnet et de les actionner à sa guise.

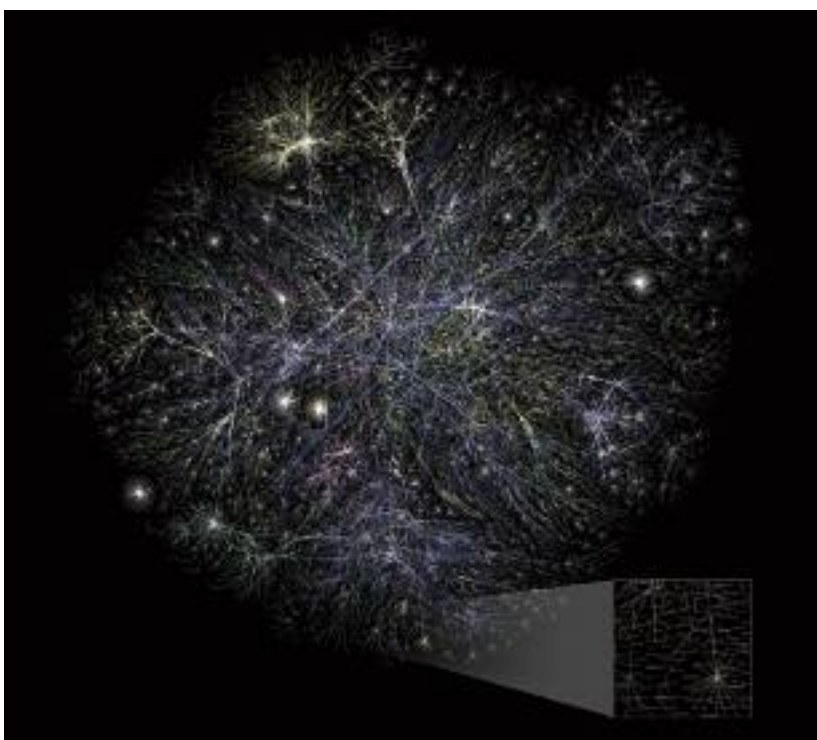
²À la conférence CanSecWest 2010, le concours PWN20WN (prononcer pawn to own, "pirater pour posséder") était doté de 100 000 US\$ répartis entre les vainqueurs qui ont pris le dessus sur le dernier iPhone 3GS d'Apple, Safari 4, Internet Explorer 8 et Firefox 3.

³<http://www.telegraph.co.uk/news/newstopping/politics/lawandorder/3173346/Chip-and-pin-scam-has-netted-millions-from-British-shoppers.html>

⁴<http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>

⁵Le filoutage (phishing) est un vol d'identités ou d'informations confidentielles par subterfuge : un malfaiteur essaie de convaincre des usagers de lui communiquer des informations confidentielles. L'utilisateur est souvent invité à visiter un site frauduleux par un courrier électronique non sollicité (spam).

⁶Peut-on encore faire confiance aux cartes réseau ?, L. Duflot et Y.-A. Perez, CanSecWest 2010, <http://www.ssi.gouv.fr/trustnetworkcard>



Visualisation des chemins multiples de l'internet : carte partielle représentant moins de 30% de l'internet existant au 15 janvier 2005 ©Matt Britt

Interopérabilité et sécurité des systèmes d'information



par **Jean-Luc Combrisson**

Ingénieur général de l'armement

Jean-Luc Combrisson est responsable du pôle télécommunications et sécurité des systèmes d'information à la direction technique de la DGA. Il est le coordinateur national des activités de recherche "SIC et réseaux" au sein de l'Agence européenne de défense et contribue aux travaux du Senior NATO Representatives Group C3 dans le domaine de la radio logicielle.

Dans le monde de la protection du secret que recouvre notamment la SSI (sécurité des systèmes d'information), on oublie quelquefois que s'il y a secret à protéger, c'est qu'il y a aussi secret à partager.

Le dilemme "sécurité vs interopérabilité"

On a souvent coutume d'opposer sécurité de l'information et interopérabilité. Il s'agit plus exactement des deux extrêmes d'une même échelle où se déplace un curseur : d'un côté le secret absolu consisterait à ne partager avec personne une information, de l'autre l'interopérabilité totale consisterait à la partager avec la Terre entière, à l'instar du modèle de mise en ligne sur internet.

Or la cryptologie s'est précisément développée pour protéger l'échange d'informations entre deux personnes (voire "N" dans le cas général) sans que d'autres y aient accès en lecture ou en modification.

Les difficultés de mise en œuvre dans les coalitions militaires

La protection du secret sur les théâtres d'opération, qu'il s'agisse d'informations tactiques (dont le temps de protection peut être très court, de quelques heures typiquement) ou stratégiques (secret à conserver plusieurs années) pose question de ce point de vue. En effet, s'il convient de protéger les informations de planification, de renseignement, de situation tactique ou d'ordres d'opérations vis à vis d'un ennemi avéré ou potentiel, il faut dans le même temps les diffuser de façon appropriée aux autres membres de la coalition.

Un risque peut en effet surgir d'une protection excessive de l'information d'une Nation A (la fameuse mention du type : "Nation A eyes only" - le "Spécial France" chez nous) ; par exemple celui de ne pas diffuser suffisamment vite la connaissance d'une menace imminente envers la Nation B, et perçue seulement par les capteurs de la Nation A. C'est également le risque pour la Nation A de ne pas diffuser la position de ses troupes à la Nation B et de conduire à des tirs fratricides. Ce risque s'est traduit par des cas réels dans les conflits récents (avion pris à partie par erreur par des avions alliés, ou troupes au sol bombardées par l'aviation amie).



Le wi-fi tu sécuriseras

Le wi-fi résidentiel (celui de la "box") doit utiliser le mécanisme WPA (bannir l'absence de chiffrement et même le mécanisme WEP qui est maintenant obsolète face aux progrès de la cryptanalyse). Cette sécurisation n'est évidemment pas possible lors de l'utilisation des réseaux wi-fi publics, sur lesquels l'information circule en clair : n'importe quelle personne située à proximité peut enregistrer vos échanges dans ce cas. Il faut proscrire tout échange de données sensibles dans cette situation, à commencer par les mots de passe, sauf si l'échange est chiffré (cadenas dans le navigateur). Il faut être extrêmement attentif aux certificats de sécurité des sites car la navigation sur réseau wi-fi public rend aisée l'interception des échanges chiffrés par un tiers qui s'interposerait sur la voie hertzienne entre l'ordinateur et les sites visités.

Ces exemples conduisent à un paradoxe sous-jacent : la protection du secret, censée assurer la sécurité de la coalition, peut conduire à une insécurité majeure.

"la protection du secret, censée assurer la sécurité de la coalition, peut conduire à une insécurité majeure"

Ce problème, connu de longue date, a bien sûr donné lieu à l'OTAN à des travaux poussés dans le domaine de l'identification (IFF), des liaisons de données tactiques (L16) et à de nombreux standards techniques d'algorithmes cryptographiques. Mais au-delà de l'adoption de standards techniques d'interopérabilité sécurisée, très longs à mettre au point, se pose toujours la question des informations qui doivent rester souveraines (le "Nation A eyes only") ainsi que de la Nation qui doit posséder la maîtrise de la distribution des clés de chiffrement et de la sécurité d'ensemble. Ces questions ne sont pas de nature technique, mais politique

: faut-il par exemple diffuser des plots radar dans une situation tactique partagée au risque de divulguer par là même les performances du radar en question, jusque là classifiées "Nation A eyes only" ? La maîtrise par une Nation A de la gestion des clés de chiffrement d'un équipement que son industrie produit permet-il néanmoins à une Nation B d'être autonome lorsqu'elle n'opérera plus avec la Nation A ? Le fait que la Nation A soit responsable de la sécurité l'autorise-t-elle à tout connaître des équipements des autres Nations ?

L'évolution des coalitions et donc des standards

L'apparition des coalitions ad hoc dans l'évolution des conflits, intégrant des Nations non-OTAN ne répondant plus à tous les standards de l'OTAN, pose de nouveau la question du choix de standards techniques d'interopérabilité et du partage de la confiance avec des alliés de circonstance.

Sur le plan technique, une certaine facilité consisterait à repousser le curseur à l'autre extrémité de l'échelle en utilisant un standard d'interopérabilité du monde civil peu sécurisé : il peut s'agir d'une radio tactique utilisée en mode clair entre deux Nations ou d'échanges via Internet pour les données. En effet, entre deux armées ne partageant pas de standards communs, la tentation est grande d'utiliser des normes civiles pour échanger de

l'information. Cependant, l'information opérationnelle mérite une protection, même au sein d'une coalition de circonstance.

De son côté, l'émergence de la cybersphère, nouveau champ de conflits, où l'information devient une cible qu'il faut défendre ou conquérir, nécessitera elle aussi des mesures permettant d'éviter des "cybertirs fratricides" entre Nations alliées.

La solution technique passe sans doute par une meilleure crypto-flexibilité, permettant de définir pour une période donnée et une coalition donnée (ou plus généralement, une communauté d'intérêt donnée) à la fois les standards de communication (IP, forme d'onde radio tactique ou Satcoms) et surtout un standard de chiffrement reprogrammable dans les équipements des membres de la coalition (radios, chiffreurs, IFF...). Une Nation doit néanmoins prendre la responsabilité de la gestion et de la distribution des éléments secrets (algorithmes, clés de chiffrement notamment). Les travaux engagés en Europe et aux Etats-Unis sur la radio logicielle offrent une voie intéressante dans cette capacité à reprogrammer une interopérabilité sécurisée au sein d'une coalition ad hoc. Néanmoins, "la confiance ne se décrète pas" et la méfiance naturelle à partager des secrets, même entre Nations proches, perdurera. Le débat sur la "position du curseur" a encore de beaux jours devant lui. ☹

Tactical Equipements

Spécialiste de l'Équipements et Accessoires
Armées - Polices - Forces Spéciales - Sécurités



Sac à Dos 3 Days - Condor



Gps Fortrex - Garmin



Poche Dual Chargeurs - Condor



Elite Spider Recon 8.0 -Magnum



Masque Locust - Revision

www.Tactical-Equipements.com

SARL TACTICAL EQUIPEMENTS
34 Rue la Foret - Local T
91860 Epinay Sous Senart
Tel: 09.81.87.09.64

Ouvert du Mardi au Samedi
10h00 - 13h00
14h00 - 19h00

Revendeur Officiel
Condor Outdoor

“High/I/Aïe!-Tech”

Quel futur pour la sécurité des systèmes d'information ?



par **Philippe Wolf**

Ingénieur général de l'armement

X78, docteur en informatique, CELAR (sécurité électronique et informatique), Directeur des études, École polytechnique, SGDSN depuis 2000, Agence Nationale de la SSI.

Merci à D. Chandesris pour l'acuité de sa vision.

1. De la convergence dans le cyber-monde

La convergence des diverses sphères du cyber-monde autour des e-services (réseaux intelligents, télétravail, télémédecine, etc.) est amorcée. Les sociétés visionnaires tâtonnent mais progressent rapidement vers des intégrations verticales : ainsi Google, opérateur d'infrastructure pour ses services, est devenu concurrent des équipementiers et des opérateurs de services ; Amazon, librairie virtuelle, est devenu fournisseur de puissance de calcul à la demande et concurrent d'IBM. On peut se rassurer en ayant constaté que les monopoles incontrôlables comme Google finissent mal en général.

Mais la convergence facilitera, à coup sûr, les modes d'action des cybercriminels

car ils s'attaquent toujours au maillon faible d'un système.

2. Des lois du cyber-monde et leurs conséquences pour la sécurité

La protection des données personnelles a beau être encadrée par la loi, force est de constater le succès des réseaux sociaux qui capturent ou, parfois, falsifient notre intimité. Le droit à l'oubli numérique se heurte à la "réalité du virtuel" : détruire une information numérique sera de plus en plus difficile. Les capacités de stockage annoncées, les outils de fouille immatérielle de plus en plus performants et les nouvelles formes de traitement de l'"informatique nébuleuse" immortaliseront le patrimoine informationnel et deviendront aussi les outils privilégiés du pillage technologique.

L'ubiquité deviendra la règle et il y a urgence à développer des normes et des outils de sécurité ouverts et interopérables pour déployer de l'informatique nébuleuse maîtrisable.

La cryptographie (voir article de G. Poupard) trouve aujourd'hui ses limites dans une gestion des clés secrètes qui nécessite une organisation rigoureuse et se satisfait mal d'une externalisation trop poussée ou d'un recours à des solutions toutes faites. Elle trouvera ses limites demain dans le très haut débit dont elle devra relever les défis (avant l'ordinateur quantique ou à ADN). Un autre de ses défis, qui est celui de l'électronique en général, sera de pouvoir travailler avec des consommations plus faibles, notamment pour le nomadisme.

Sécurité et confiance numériques

Le cyber-monde actuel

Quatre sphères technologiques en réseaux "rhizomiques" :

- la sphère de l'Internet peu régulée, assez friable car reposant sur un squelette momifié (TCP/IP en 1983) même si très résiliente avec des capacités d'extensions vers le très haut-débit (record de transmission sur 7000 km de fibre optique : > 100 pétabits/s = 10^{12} bps), champ privilégié des attaques informatiques vecteurs d'une nouvelle activité souterraine de plus en plus lucrative ;
- la sphère des technologies mobiles très contrôlée par les opérateurs nationaux et globaux, plus fragile avec des limitations physiques (la barrière des 100 Mbit/s en radio sera difficile à franchir) et une bataille fœutrée autour de la gestion future des fréquences qui resteront une ressource rare et stratégique ;
- la sphère de la géolocalisation sous contrôle des quelques États en capacité de la déployer : GPS américain et GLONASS russe disponibles aujourd'hui, systèmes européens et chinois dans quelques années ; elle s'incruste dans nos objets quotidiens et parfois déjà dans le corps des êtres vivants ;
- la sphère du nouvel Internet des objets dont les enjeux de contrôle sont très importants et vraisemblablement futur champ d'attaques rendues possibles par une sécurisation faible liée aux coûts.

En 5000 ans d'histoire non numérique, l'humanité a généré l'équivalent de 5 exaoctets (10^{18}) d'information.

Poussé par la haute définition, la 3ème dimension et les contenus générés par les utilisateurs, le volume annuel de l'information numérique va bientôt atteindre 1000 exaoctets soit 200 fois plus.

Dans un article célèbre publié en 1984 (Reflections on Trusting Trust), Ken Thompson montre comment piéger nativement un ordinateur en créant une porte dérobée quasiment indétectable. Il conclut sa démonstration ainsi : "La morale est évidente. Vous ne pouvez pas faire confiance à du logiciel que vous n'avez pas totalement créé par vous-même. En particulier, ne faites pas confiance à des sociétés employant des types comme moi". Les possibilités de piégeage, en combinant les couches physiques, syntaxiques et sémantiques, sont infinies.

Pour pouvoir parler de souveraineté numérique, il faudra en maîtriser les techniques.

Mais ni la France, ni même l'Europe ne sont aujourd'hui entièrement maîtres des

technologies alors que les quelques pays qui affirment clairement un concept de "suprématie informationnelle", comme les États-Unis ou la Chine (le futur G2 des systèmes d'information ?), se donnent, parfois difficilement, les moyens de maîtriser l'ensemble des briques technologiques des outils qu'ils déploient. Et on nous annonce la convergence "nano-bio-info-cogno" dont les implications éthiques et sociales font déjà l'objet de recherches.

3. De l'Internet des objets : Small Brother au lieu de Big Brother ?

L'Internet des objets rendu possible par l'IPv6 a pour but d'étendre le réseau au monde réel en associant des étiquettes munies de codes aux objets ou aux lieux. Ces étiquettes, utilisant la technologie RFID, pourront être lues par des dispositifs

mobiles sans fil ou des bornes fixes. Nous en avons déjà dans nos poches aujourd'hui (clef vigik des immeubles d'habitation, pass navigo pour les transports, passeport biométrique, etc.). Si la traçabilité est bien vue par l'acheteur pour les produits alimentaires, elle pose de nombreux problèmes lorsque l'on se rapproche des êtres humains et de leur mode de vie. La finesse de traçage sera proportionnelle au maillage des portiques de lecture (composteur, porte d'entrée, caisse de supermarché, affiches publicitaires, téléphones mobiles, etc.). Le législateur invoque le "silence des puces" comme une garantie de non traçabilité. Mais il est techniquement impossible de doter un objet passif d'un bouton marche-arrêt.

Des milliards d'étiquettes se promèneront avec et autour des êtres humains et seront

Les mises à jour de sécurité sans délai tu appliqueras sur tous tes logiciels

La correction sans délai des failles de sécurité des logiciels est la plus importante des mesures de protection contre les attaques informatiques. Les mises à jour du système d'exploitation doivent être appliquées automatiquement ; les mises à jour des autres logiciels doivent être activées automatiquement si c'est possible, fréquemment recherchées à la main sinon. L'utilisation d'un utilitaire spécialisé, tel que Secunia PSI par exemple, permet de signaler automatiquement les logiciels à mettre à jour et les failles de sécurité majeures.



Quelques lois du cyber-monde

Trois lois exponentielles croissantes caractérisent l'expansion du monde numérique. La loi de Moore (1965) affirme que la complexité des semi-conducteurs double tous les dix-huit mois à coût constant, la loi de Gilder affirme que la bande passante des réseaux double tous les neuf mois et la loi empirique de Metcalfe affirme que l'utilité (pour les vendeurs ?) d'un réseau croît comme le carré du nombre de ses utilisateurs. Les développements logiciels ou micro-logiciels suivent eux la loi de Hofstadter qui déclare que : "Ça prend toujours plus de temps qu'on croit, même en prenant en compte la loi de Hofstadter". Ainsi, les vulnérabilités de machines de plus en plus complexes soumises à des impératifs de rapidité de mise sur le marché vont croître dans une proportion incommensurable. Confrontés à une réalité finie, ces lois s'infléchiront ; on parle d'une rupture dans 20 ans pour la loi de Moore, une cyber-éternité...

détectées plusieurs fois par jour par plusieurs centaines parmi les millions de détecteurs.

L'industrie deviendra de plus en plus dépendante de ces puces pour ses approvisionnements, sa fabrication, sa gestion de stocks, sa traçabilité. Les risques sur l'infrastructure (piratage, saturation des données, usurpation des droits) sont classiques. Les risques dus à la possession de l'infrastructure par un tiers sont moins visibles mais bien réels. Il existe un "Object Name Server (ONS)" équivalent du "Domain Name Server (DNS)" d'Internet entièrement administré aux États-Unis (en 2004, la société VeriSign a gagné un contrat lui permettant d'opérer un ONS pour le consortium EPCglobal). Cet ONS centralise les informations sur les étiquettes (produit fabriqué par X à la date A, distribué par Y à la date B, acheté

par Z à la date C...). Celui qui contrôle cet ONS peut tracer les produits étiquetés mais aussi leurs acheteurs/utilisateurs, qu'ils soient des personnes physiques ou morales. Les problèmes de gouvernance de l'Internet des objets vont se poser dans des termes très proches de celui de l'Internet.

Une société trop numérique se fragilise alors même que les objets communicants et intelligents vont se multiplier et envahir notre quotidien.

Dans un livre de 1999 intitulé en français "La Guerre hors limites" les auteurs déclaraient : "Nous croyons qu'un beau matin les hommes découvriront avec surprise que des objets aimables et pacifiques ont acquis des propriétés offensives et meurtrières". Ainsi, une attaque informatique sur un congélateur

intelligent branché sur l'Internet pourrait rompre discrètement la chaîne du froid lors des vacances de son propriétaire, dans un objectif d'empoisonnement de celui-ci.

4. De la nouvelle sécurité des systèmes d'information

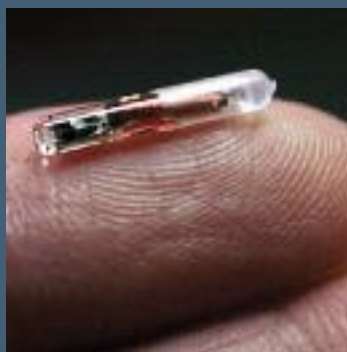
Aujourd'hui encore, le modèle de protection des systèmes d'information considère des boîtes interconnectées et c'est à l'utilisateur d'y ajouter des fonctions pour se protéger (firewall, antivirus, contrôleur d'intégrité, chiffrement de disque). Demain, et l'on constate cela au vu de la confiance parfois aveugle en la technologie de la génération qui a grandi avec le numérique, le modèle sera celui d'offres de services complètement intégrés, au niveau de sécurité adéquat, sans que l'utilisateur n'ait à s'en

Le protocole IPV6

Le protocole IPV6 (successeur du vieux protocole IPV4 qui forme encore en 2010 l'ossature d'Internet) a défini en 1995 un adressage sur 128 bits ($2^{128} = 3,4.10^{38}$ adresses). Cela fournit théoriquement 7.10^{23} adresses par m² sur Terre (terre + eau, un nombre supérieur au nombre d'Avogadro). Même en réservant la moitié (seulement !) des adresses pour le monde extraterrestre et en prenant en compte des contraintes de nommage, cela fournit, dans le pire des cas prévisibles, 1500 adresses au m², de quoi construire l'Internet des objets.



La radio-identification



La radio-identification désignée par le sigle RFID (Radio Frequency Identification) est une méthode pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés "radio-étiquettes" ou "RFID tag". Les radio-étiquettes sont de petits objets, tels que des étiquettes autoadhésives, qui peuvent être collées ou incorporées dans des objets ou produites et même implantées dans des organismes vivants (animaux, corps humain). Les radio-étiquettes comprennent une antenne associée à une puce électronique qui leur permet de recevoir et de répondre aux requêtes radio émises depuis l'émetteur-récepteur. Ce sont des dispositifs passifs, ne nécessitant aucune source d'énergie en dehors de celle fournie par les lecteurs ou bornes au moment de leur interrogation (qui peut être faite de quelques centimètres à quelques dizaines de mètres).

préoccuper. Seul le prescripteur et le fournisseur, voire l'inspecteur contrôlant les contrats de services, se soucieront de la sécurité des systèmes d'information, comme c'est le cas de la sécurité automobile ou de l'achat immobilier. Il sera fait appel à des spécialistes qu'on espère de confiance, dont le métier sera de surveiller, détecter, analyser des signaux faibles, corrélés des incidents mineurs pour opérer la sécurité.

Il faudra également mieux tenir compte de l'hétérogénéité des besoins de protections et des perceptions aux agressions. Pour les personnes, il faudra proposer à la fois une meilleure identité numérique (agacement des pourriels, protection des espaces privés) et des fonctions d'anonymat ou de "pseudonymat", à l'image des avatars virtuels que se créent les joueurs en réseau, qui favoriseront la liberté d'expression dans les pays opprimés mais aussi l'impunité des criminels (ambivalence naturelle des fonctions de sécurité). La sécurité des systèmes des entreprises et des organisations ne pourra plus être uniforme : cloisonnement mou en cas de coopération, cloisonnement fort en cas de compétition ou de perception de vol de

technologie, de clientèle ou d'image (déstabilisation).

Sur le plan juridique, Internet, souvent présenté comme un espace de non-droit, va se structurer en zones plus homogènes dont le modèle de protection des systèmes d'information reflètera le modèle de société et les valeurs de chaque zone : modèle libéral nord-américain (la liberté fonde la société), modèle chinois (l'organisation fonde la société), modèle européen où la protection du faible est plus prise en charge par l'État (la dignité fonde la société). Dans le registre de la souveraineté, des jeux étranges, parfois pusillanimes, se jouent déjà et se joueront : émancipation du contrôle américain de l'Internet par la Chine, déclarations de capacités offensives en la matière (USA...), volonté de désarmement (Russie qui n'a, par contre, pas signé la convention de Budapest sur le cyber-crime), affrontements asymétriques sourds, paradis numériques.

5. De l'État

Une proposition de loi du Sénat visant à mieux garantir le droit à la vie privée à

l'heure du numérique et s'appuyant sur un rapport qui "appelle de ses vœux la transformation de l'Homo Sapiens en un Homo Numericus libre et éclairé, protecteur de ses propres données" considère que toute adresse IP est une donnée à caractère personnel. Sans discuter du caractère irréaliste et inefficace de ce principe et de la crainte de la disparition de l'homme sage, il ouvre la porte à un anthropomorphisme des systèmes d'information dont on ne peut mesurer aujourd'hui toutes les conséquences. Le premier défi de la future sécurité des systèmes d'information sera bien la protection de cet homme numérique dont la volonté seule ne saura suffire. Le rôle de l'État sera aussi de paver toutes les évolutions numériques en organisant les stratégies de régulation, en gérant son monopole de répression du cybercrime, en maintenant une compétence humaine et technique forte grâce au développement de la formation et de la recherche en sécurité des systèmes d'information. ☞

Franche-Comté : l'exigence industrielle pour la défense et l'armement

EUROSATORY

Hall 6
Stand EF 373



signed Franche-Comté®

145 entreprises développent leurs savoir-faire pour la défense et l'armement, là où la miniaturisation, l'aptitude à s'intégrer à des environnements extrêmes et l'intelligence prennent toujours plus d'importance. Plusieurs marchés de niches sont exploités, notamment les connecteurs simples et multibroches, les contacteurs et voyants, des instruments de bord, des équipements de contrôle non destructif, des systèmes de sécurité embarqués d'armement des fusées....

Les compétences industrielles s'appuient en Franche-Comté sur un **important pôle de recherche** et notamment sur l'Institut FEMTO-ST. Fort de ses 500 chercheurs, l'Institut développe ses activités de recherche autour de plusieurs axes qui intéressent spécialement la défense, et notamment la microfabrication, les micro et nano systèmes, de la microanalyse des surfaces et les projets appliqués au temps-fréquence et aux télécommunications.

L'ARES (Association Recherche Économie Sciences) soutient le développement des PME régionales sur le marché de la défense en impulsant leur diversification au service de ce marché exigeant.

A VOIR EN 2010 SUR LE COLLECTIF FRANCHE-COMTÉ

- **AR ELECTRONIQUE**, acteur majeur dans le domaine des dispositifs temps-fréquence. Une gamme particulièrement étoffée d'oscillateurs développés soit en version professionnelle et en version militaire. ISO 9001 - 2000.
- **BAUDRY**, partenaire de la défense dans les techniques de protection et de conditionnement. ISO 9001 - 2000, agréé par l'OTAN sous le n° F8252.
- **BECKER ELECTRONIQUE**, filiale du Groupe Becker Avionic Systems, systèmes électroniques allant de la carte manufacturée jusqu'au produit complet. Une gamme complète de systèmes de communication embarqués. ISO 9001 - 2000, agréé EADS, EASA, BVB.
- **DIXI MICROTECHNIQUES**, fournisseur des principaux groupes munitionnaires européens. Dispositifs microtechniques de sécurité ou de mise à feu pour munition, équipements de sécurité pour systèmes embarqués. Référencé EADS, THALES, NEXTER.
- L'Institut Pierre **VERNIER**, centre de transfert de technologies, travaille pour nombre de grands comptes du secteur aéronautique / défense (THALES, SNECMA, SOURIAU, CEA, ...) et pour leurs sous-traitants.
- **PRECLJURA**, décolletage et micromécanique de très haute précision, dans tous les matériaux usinables à l'outil, du ø0.50 à 42 mm.

www.salons.franche-comte.cci.fr
www.franche-comte.cci.fr
www.cciexpert.net

Contact :
Stéphane Angers - CROI Franche-Comté
Tél. + 33 (0)3 81 47 42 00
Fax + 33 (0)3 81 80 70 94
salons@franche-comte.cci.fr

 Franche-Comté
Conseil régional

 CHAMBRE RÉGIONALE
DE COMMERCE ET D'INDUSTRIE
DE FRANCHE-COMTÉ

Quelle protection face aux cybermenaces ?

Cyberdéfense : un exemple de solution déployée



par **Christophe Dumas**

Ingénieur en chef de l'armement

Directeur de la stratégie de la division

Systèmes C4I de Défense et Sécurité du groupe Thales

Avant de rejoindre THALES en 2002, Christophe Dumas a occupé au sein de la DGA des postes de maîtrise d'ouvrage de développement de systèmes d'information opérationnels, de coopération internationale, de tutelle de l'industrie aéronautique, puis de chef de cabinet du Délégué.



par **Stanislas de Maupeou**

Colonel (er) de l'armée de Terre

Responsable de l'offre Cyber-défense Division Systèmes C4I

de Défense et Sécurité du groupe Thales

Avant de rejoindre Thales en 2009, Stanislas de Maupeou a été chef du centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques (CERTA). Avant ce détachement au sein du SGDSN, il a été officier des troupes de marine.

Sécuriser le cyberspace est vital pour le bon fonctionnement de nos sociétés : c'est déjà un champ d'affrontement, il sera peut-être un jour utilisé comme une arme. Dans ce contexte, la cyberdéfense n'est pas un effet de mode et les cybermenaces ne sont pas une fatalité, mais un enjeu majeur pour nos sociétés de l'information face auquel des solutions éprouvées existent.

Vers une défense active

La protection des systèmes d'information sensibles a toujours été au cœur des préoccupations des organisations de défense et de sécurité. Cependant, cet enjeu a ces dernières années changé de nature,

du fait des transformations profondes induites par l'explosion des nouvelles technologies de l'information et des communications. Le bon fonctionnement des États et des entreprises est de plus en plus dépendant de systèmes d'informations interconnectés. Et cette interconnexion

facilite la propagation des attaques, dont les occurrences ne cessent d'augmenter. Des organisations étatiques ou pas multiplient les postures agressives sur les réseaux.

C'est pourquoi le Livre blanc sur la défense et la sécurité nationale insiste dans sa

Les informations sensibles tu chiffreras

L'envoi de données personnelles sensibles sur des sites internet ne doit se faire que si la communication est sécurisée (cadenas dans le navigateur). Pour les autres données, l'utilisation d'utilitaires de chiffrement fournis par l'entreprise ou installés à partir d'une source sérieuse, de préférence labellisés par l'ANSSI (le logiciel libre TrueCrypt par exemple), permet de réduire le risque de compromission de l'information en cas d'intrusion dans le système ou d'interception des échanges, pour autant que les clés de chiffrement ou mots de passe soient longs et non-prédictibles.



Le mythe tenace de la cyber-ligne-Maginot

On entend encore trop souvent dire : "je suis protégé parce que mon réseau n'est pas interconnecté à l'Internet". Comme l'a montré en 2009 la propagation d'un code malveillant au sein des réseaux du ministère de la Défense (mais pas uniquement), cette défense strictement périmétrique est illusoire au regard de la réalité des interconnexions cachées ou peu maîtrisées (clef USB, ordinateur portable, Smartphone, etc.) et face à la sophistication des attaques.

dernière édition sur la nécessité de mettre en œuvre une capacité centralisée de détection et de défense face aux attaques informatiques.

Il s'agit de dépasser l'approche traditionnelle de "défense passive" de type "ligne Maginot" où les systèmes d'information sensibles étaient protégés des attaques par des barrières physiques (locaux sécurisés) et logiques (pare-feux, filtres, mots de passe) dressées tout autour d'eux. Cette approche n'a d'ailleurs plus guère de sens compte tenu du recours croissant à l'externalisation des infrastructures informatiques ("cloud computing").

La sécurisation de systèmes ouverts et interconnectés nécessite désormais une approche de défense active en profondeur, reposant sur la détection la plus précoce possible des cyber-attaques.

La cyberdéfense constitue ce passage d'une défense passive à une défense active qui évalue en temps réel l'exposition d'un système d'information à des cyber-attaques.

Supervision de sécurité : un retour d'expérience industrielle

L'industrie n'a pas tardé à bâtir une offre de cyberdéfense. A titre d'exemple, Thales opère depuis dix ans un centre permanent de supervision de la sécurité des systèmes d'informations sensibles d'infrastructures

vitales dans le monde de la banque, du transport ou de l'énergie.

Au fil du temps, Thales a combiné cette expérience de service de cyberdéfense à son expertise unique dans la conception et le développement des produits de haute sécurité afin de développer une offre globale de cyberdéfense : CYBELS (CYBer Expertise for Leading Security).

L'offre CYBELS se décline selon trois modes complémentaires :

- la supervision 24 heures sur 24 d'un système d'information (opérée pour le compte d'un client) selon des procédures normées ;
- la fourniture de capacités de cyberdéfense comme par exemple l'hypermision de

différents systèmes sous surveillance, la formation d'experts destinés à servir dans un centre de cyberdéfense ou encore la mise en œuvre de moteurs de corrélation d'événements ;

- la fourniture d'un centre opérationnel de cyberdéfense "clef en main" (permettant au client d'assurer par lui-même la cyberdéfense de son système d'information). Le centre opérationnel de cyberdéfense permet d'orchestrer un ensemble complet de capacités de cyberdéfense et d'en assurer la cohérence :
- détection des attaques à partir de sondes judicieusement placées au sein du système d'information ;
- collecte des informations issues des journaux d'événements générés par tous





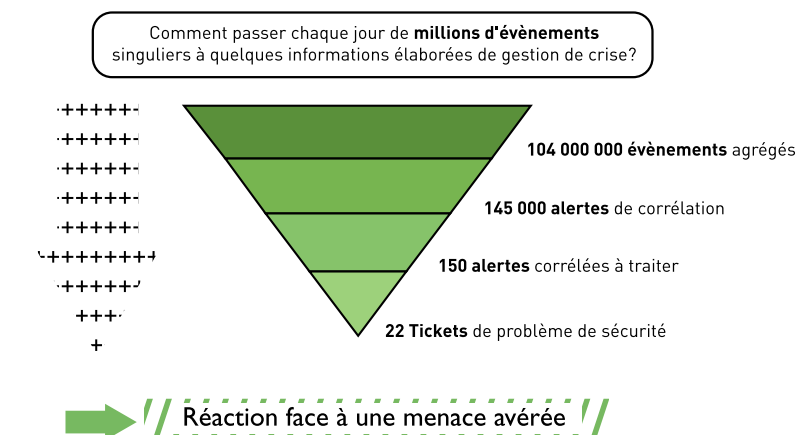
les composants d'un système ;

- corrélation et mise en perspective de toutes les informations ainsi collectées afin d'établir des "tickets d'incidents" qui peuvent donner lieu à une alerte de sécurité ;
- analyse des informations construites et pilotage de la réponse opérationnelle en lien avec le client.

Ces étapes majeures de cybersécurité ne peuvent se concevoir sans procédures techniques et mesures d'organisation au sein du centre opérationnel de cybersécurité : relevé des ingénieurs de quart, gestion des tickets d'incidents, traçabilité des actions, anticipation des nouvelles menaces, coopération internationale, stockage des informations collectées, respect du cadre juridique, habilitation des équipes, contrôle interne, etc... Cette complexité propre à tout centre opérationnel est particulièrement vraie dans le cyberspace du fait de la densité des trafics et des volumes d'informations à traiter quotidiennement (cf. figure ci-contre).

L'impérative nécessité du maintien en condition de sécurité

Tout ce travail de détection, de corrélation, d'analyse et de pilotage n'a de sens que dans la mesure où l'on connaît l'état de son parc (les versions des logiciels, les configurations, les architectures) et que l'on est capable d'appliquer un correctif de sécurité ou bien une mesure palliative (par



exemple : modification d'un paramètre pour rendre une attaque inopérante).

La cybersécurité repose donc également sur la capacité à garantir et à maintenir dans le temps un niveau de sécurité. Cette exigence de maintien en condition de sécurité (MCS) est d'autant plus nécessaire que les cyber-attaques exploitent des vulnérabilités pour se propager. Au moment où cet article paraît, il a été publié sur l'internet plus de 2 000 vulnérabilités depuis le début de l'année 2010 !

Thales met en œuvre une offre et des outils de maintien en condition de sécurité afin de garantir qu'au cours du temps, les conditions de sécurité qui ont conduit à homologuer un système d'information à un instant donné sont toujours réalisées. Cette

capacité est le fondement de la cybersécurité, elle en constitue la pierre angulaire.

Conclusion : face à des menaces bien réelles, des solutions éprouvées existent

Si les menaces et les enjeux du cyberspace font l'objet de toutes les attentions, la réalité opérationnelle de la cybersécurité est plus méconnue. En effet, construire un centre opérationnel de cybersécurité puis opérer un service permanent de supervision requiert des expertises et des savoir-faire rares. C'est d'ailleurs ce qui fait toute la valeur des offres complètes de cybersécurité comme CYBELS. 🛡️

La cybersécurité peut être définie comme l'ensemble des actions coordonnées de prévention, d'analyse et de réaction aux cyber-attaques visant à se protéger de façon permanente et la plus précoce possible des menaces pesant sur un système d'information. Dans ce contexte, la cybersécurité contribue à la résilience des organisations en apportant des capacités d'anticipation et de réaction rapide face à des agressions intentionnelles ou accidentelles.

Des technologies de l'ingénieur aux sciences du vivant

Bertin Technologies est un des leaders de l'innovation industrielle avec une offre unique d'expertises et d'équipements à fort contenu technologique. Depuis plus de 50 ans, fidèles à nos principes d'écoute, d'excellence technique et de professionnalisme, nous mobilisons le talent de nos équipes et tout notre capital technologique pour accompagner nos clients. Nous poursuivons notre croissance à l'international et investissons durablement dans la Recherche et l'Innovation.

Direction du Développement
Tél. +33 (0)1 39 30 61 50
www.bertin.fr

bertin
TECHNOLOGIES
LA MAÎTRISE DE L'INNOVATION

Société du Groupe
ENIM

Energie & Environnement

Défense & Sécurité

Aéronautique & Espace

Industries & Services

Sciences du vivant

Mai 2010



Conseil et Expertise en Sécurité des Technologies de l'Information

AMOSSYS est une société indépendante spécialisée en Sécurité
Jeune Entreprise Innovante

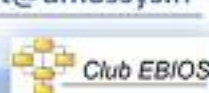
Nos domaines d'intervention

- ✓ L'évaluation de la sécurité
 - CESTI en cours d'agrément
 - Centre d'Évaluation CSPN
- ✓ Les études amont, la R&D appliquée
- ✓ Le conseil et l'assistance
- ✓ L'audit de la sécurité
- ✓ La formation en SSI

Exemples de travaux

- ✓ Analyse de Sécurité de Défense (Ministère de la Défense) Réalisation d'évaluations de produits de sécurité reposant sur le référentiel CSPN de l'ANSSI.
- ✓ Membre « contributeur » du *Trusted Computing Group*, groupe de réflexion spécifiant les nouvelles technologies de l'informatique de confiance.

contact@amossys.fr



Sécurité et confiance numériques

Le passeport biométrique, la sécurité numérique dans votre poche



par **François-Xavier Fraisse**

Ingénieur en chef de l'armement
Directeur de programme, Sagem Sécurité

X85-Armement, François-Xavier Fraisse a une double expérience DGA technique (guidage-pilotage de missiles au LRBA) et internationale (chef de bureau géographique, chef de cabinet du DRI, chargé de mission auprès du représentant personnel du ministre). Il a rejoint Sagem Sécurité en 2001 où il a été chef de programme de systèmes d'identification puis directeur de programme des visas puis passeports biométriques français. Il dirige actuellement une offre de PPP (partenariat public privé).

Depuis juin 2009, les passeports français intègrent l'empreinte digitale numérisée de leur porteur. Au-delà de la modernisation et de la sécurisation des processus, des nouveaux services vous deviennent accessibles.

Une vision politique et un champ réglementaire européen

Depuis de nombreuses années le ministère de l'intérieur étudiait le renforcement de la lutte contre la fraude à l'identité, la modernisation de la chaîne de traitement des documents d'identité et la mise en place de nouveaux services au citoyen. Une agence dédiée a été instaurée en 2007 (agence nationale des titres sécurisés ou ANTS), avec des moyens assis sur les droits perçus sur la délivrance des titres. La réglementation européenne imposant la mise en place d'un passeport biométrique à compter de juin 2009 a contribué à déclencher le projet TES (titres électroniques sécurisés).

Concrètement il a été décidé d'équiper

plus de 2000 mairies et 200 Consulats de terminaux permettant la saisie dématérialisée des demandes, ce qui permet de réduire les délais de collecte et transmission des demandes ainsi que d'optimiser l'organisation du travail en Préfectures. Un projet clé de la RGPP (refonte générale des politiques publiques), mais aussi un important travail de gestion du changement...

Un calendrier contraint mais une forte exigence de sécurité

Le marché TES a été notifié tardivement, 12 mois avant la date d'échéance européenne. Les deux co-contractants (Sagem Sécurité et Atos Worldline) ont donc engagé une véritable course contre la montre, en gérant différents fronts de

développement logiciels, production d'équipements, déploiement et formation. La tenue d'exigences de sécurité non négociables était liée :

- à la protection des données personnelles des demandeurs. Aucune fuite ne doit être possible au niveau des stations de saisie, des transmissions et du système central. Un réseau virtuel protégé (VPN) a par exemple été constitué pour relier l'ensemble des mairies au site central.
- au strict contrôle des accès des agents en Mairie, Préfecture ou Consulat, nécessitant par exemple la distribution de cartes à puce avec certificat de signature, préfigurant d'ailleurs les futures cartes nationales d'identité électroniques. Les prescriptions très précises de la CNIL ont été contrôlées au cours d'une recette réalisée en présence de l'ANSSI,

Tes données fréquemment tu sauvegarderas

Il est essentiel de conserver hors de son disque dur une copie de ses données afin de pouvoir se prémunir de toute perte définitive suite à une attaque ou un dysfonctionnement informatique.



“Remise du premier passeport biométrique français par Michèle Alliot-Marie et Eric Woerth, alors respectivement ministres de l’intérieur et du

permettant de constater que la rapidité du projet n’était pas synonyme de relâchement de la rigueur !

Quels bénéfices pour le citoyen ?

Les premiers bénéfices sont déjà visibles : possibilité de réaliser une demande de passeport dans n’importe quelle mairie (plus uniquement celle du lieu de résidence) et ouverture progressive de portes automatiques (“smartgates”) aux frontières permettant le passage accéléré à l’entrée/sortie de l’espace Schengen. L’accès à l’empreinte digitale stockée dans la puce électronique du passeport est protégé par un mécanisme “extended access control” (EAC) qui limite son usage aux Etats européens avec lesquels la France partage les certificats ad-hoc.

Au-delà s’ouvre la perspective rapide des services de la future carte nationale d’identité électronique (CNIe) pour laquelle l’infrastructure de demande et de délivrance est déjà en place.

Quelles différences avec un programme d’armement ?

Le domaine de la sécurité se caractérise par des constantes de temps excessivement courtes. Il n’est pas question de gérer des ruptures technologiques, mais plutôt d’implémenter au mieux des solutions éprouvées.

Le financement des frais de R&D par l’Etat est limité, ce qui impose d’optimiser les solutions avec une modularité permettant la réutilisation des composants sur de nombreux marchés.

Par ailleurs, les contraintes de visibilité et d’acceptabilité par le grand public, les agents et les élus locaux sont particulièrement dimensionnantes : par exemple il n’est pas acceptable qu’une empreinte digitale non cryptée soit retrouvée sur un disque dur en mairie ou qu’un voyageur se voie signifier la veille de son départ que sa demande de passeport a été malencontreusement effacée par le système... Les programmes de sécurité se retrouvent très rapidement sous le feu des projecteurs, avec des phases pilote et de recette très courtes. Beaucoup de contraintes, mais au final la satisfaction de pouvoir constater en moins d’un an des changements dans le quotidien de nos concitoyens ! 📢

Sécurité et confiance numériques

Pour une politique industrielle dans le domaine de la sécurité des systèmes d'information



par **Luc Renouil**

Ingénieur principal de l'armement
Directeur du développement, Bertin Technologies

Après un début de carrière à la DGA puis à Bercy, l'auteur a participé au redéploiement et au développement de Bertin Technologies, acteur majeur de l'innovation produit pour la Défense, les Biotech, l'Environnement. Bertin est à l'origine de Polyxène, un système d'exploitation gouvernemental certifié et de confiance.

Quelles innovations industrielles peuvent permettre avec les moyens disponibles d'avoir des réponses en termes de SSI ? L'auteur essaye d'aborder la question à la fois sous l'angle de la réflexion et des propositions.

L'auteur remercie Emmanuel Gureghian, responsable des activités en Sécurité des systèmes d'Information pour ses réflexions essentielles à la rédaction de cet article.

La SSI c'est bien plus que la crypto

La part de la cryptographie dans la SSI s'est réduite alors qu'elle en constituait la majeure partie jusqu'au milieu du XX^{ème} siècle. Elle se place désormais en support d'autres mécanismes tels que l'authentification ou le contrôle d'accès.

La standardisation de l'informatique et des protocoles de transmission a permis de développer des usages nouveaux notamment en matière d'accès mobile aux données, de dématérialisation de procédures... auxquels tout utilisateur ou toute organisation ne peut rester insensible. Mais ces nouveaux usages posent la question de la maîtrise de ces technologies et des risques associés.

Le Livre blanc sur la défense et la sécurité nationale l'a souligné (et des attaques comme celles contre l'Estonie l'ont confirmé), la menace informatique est maximale et il faut que la France se prépare à cette fin, sur la base d'une analyse stratégique saine, notamment en entretenant une base

industrielle renouvelée.

Nous essayerons d'aborder dans la suite la question de la cyberdéfense en portant un regard industriel intéressé à la question et au marché.

Schématiquement, la situation dans le domaine des systèmes d'information (SI) n'est pas la même que dans l'aéronautique où nous disposons encore de la possibilité de créer et produire nos propres avions. Du matériel au logiciel en passant par les télécommunications, le secteur est dominé par les acteurs asiatiques (composants, assemblage, bientôt équipements de réseaux) et américains (processeurs, logiciels).

Au vu de ces constats, qui se traduisent par une confiance limitée attribuée aux machines et à leurs logiciels, la sécurisation des SI a jusqu'alors été essentiellement basée sur la sécurité périmétrique, ce qui signifie qu'une machine est intégrée physiquement à un réseau dont tous les accès sont contrôlés. La manipulation des données confidentielles est limitée à des zones physiquement sécurisées.

Une telle stratégie de sécurité, interdisant tout emploi de type nomade ou ouvert en interopérabilité, semble désormais difficilement tenable pour les futurs systèmes de la Défense comme pour ceux qui sont critiques pour la sécurité de l'Etat (moyen de transport, de production de l'énergie...). Elle est de plus très vulnérable : dès qu'un logiciel malveillant réussit à s'introduire dans le périmètre sécurisé (clé USB, pièce jointe infectée...), la sécurité s'effondre.

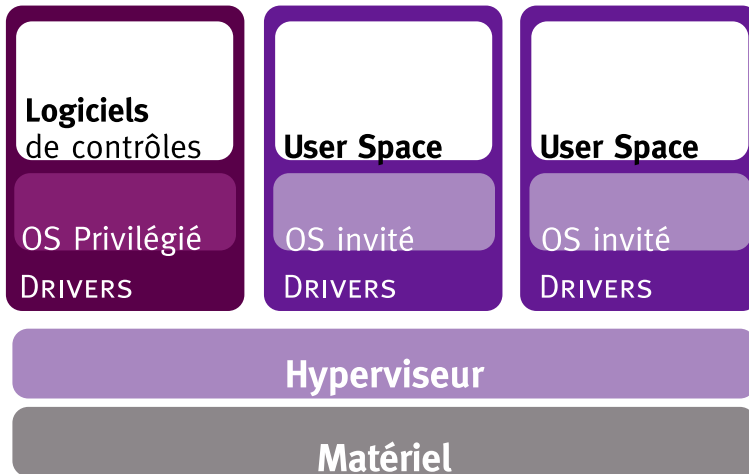
Comment passer de la ligne Maginot à une vraie stratégie de défense dans la profondeur, seule garante d'une réelle sécurité, en répartissant, selon les SI, les défenses du centre à la périphérie ?

Quand on n'a pas de pétrole, il faut avoir des idées, et les mettre en œuvre

Le cas du système d'exploitation (OS) est intéressant, car cette première couche logicielle est critique puisqu'elle contrôle un matériel dont on a vu précédemment qu'il ne

Tes informations personnelles tu veilleras

L'internet n'est pas discret et les informations que l'on y laisse échappent à tout contrôle ultérieur. Les informations personnelles et sensibles ne doivent être confiées qu'à des sites de confiance, de préférence utilisant des connexions sécurisées, et jamais à des forums publics. Les réseaux sociaux, en particulier, doivent être utilisés avec prudence même lorsqu'on croit pouvoir limiter la diffusion des informations que l'on y insère.



peut être considéré comme de confiance étant donné sa non-maîtrise par l'industrie nationale. De plus, si le système d'exploitation contrôle le matériel (accès, gestion), il implante aussi des mécanismes de sécurité critiques qui sont systématiquement invoqués : confinement des données en mémoire, cloisonnement des parties logiques du système, contrôle d'accès, intégrité des logiciels.

Si on observe les éléments de domination dans le domaine industriel des technologies de l'information, ceux qui sont de nature à fixer un paysage industriel, les OS sont de l'ordre de la suprématie. Que seraient Microsoft sans Windows ou Sun sans Unix ? D'où la stratégie technique consistant à promouvoir une source d'OS de sécurité gouvernementale, en tirant partie des avancées technologiques, notamment en terme de virtualisation.

Il n'est pas envisageable de développer complètement un OS souverain, en raison des coûts de développement et de la nécessité d'interopérabilité avec les SI préexistants. Il s'agit tout d'abord de tirer parti de la maturité de certaines technologies pour développer des fonctionnalités avancées notamment de sécurité, ensuite de partager cette démarche pour fabriquer des solutions de sécurité implantable dans la profondeur de nos réseaux.

Sur le premier point, les fonctions de sécurité

implantées doivent prendre en compte les nouveaux usages et les nouveaux besoins (mobilité ou nomadisme) et être en mesure de fournir des capacités de connexion sécurisée entre réseaux.

Sur le second point, l'effort est relié à l'exploitation de processeurs de plus en plus coopératifs en matière de sécurité. Cela a été le sujet du projet Plateforme de Confiance du pôle de compétitivité Systematic, et d'autres initiatives existent dans des projets européens. La communauté en cours de création sous l'égide de l'ANSSI permettra aussi clairement de mettre en commun les efforts gouvernementaux français pour développer ces logiciels sécurisés dont les utilisateurs de solutions de confiance français et européens ont besoin.

Windows ou Linux telle n'est plus vraiment la question, mais l'Europe est bien la question

La vraie question pour un tel OS reste l'interopérabilité avec les SI préexistants ou futurs, notamment au regard des marchés visés et des règles de propriétés qui existeront sur ces logiciels. Il y a de ce côté-là une gageure. D'une part, le marché visé ne peut se limiter au besoin gouvernemental de la Défense française, car le coût pourrait s'avérer difficile à supporter pour elle. Il convient de considérer le marché européen du logiciel de

sureté pour la Défense, l'Aéronautique, le Transport et l'Energie. On parle d'un marché de plusieurs milliards d'euros annuels. C'est à ce niveau qu'attaquent les concurrents américains, fournisseurs de solution de virtualisation. C'est au niveau européen qu'il faut fédérer les efforts pour construire une base industrielle et technologique.

Par ailleurs, la logique du tout logiciel libre peut se défendre quand il n'y a pas trop de contrainte d'interopérabilité internationale. Cela pouvait paraître une hypothèse séduisante il y a quelques années (quand nous avons lancé nos projets). Désormais, il semble que, pour le ministère de la défense, l'importance des opérations OTAN oblige au pragmatisme et à la compatibilité avec le grand système d'exploitation qui restera Windows, dans sa version 7 notamment, qui a des hypothèses dimensionnantes par rapport à certains points de sécurité informatique. Pour mener une stratégie de coopération sans suivisme excessif de Microsoft, le niveau européen sera sans doute le bon niveau. Pour cela il conviendra aussi que les instances gouvernementales se concertent pour participer à la construction des projets, des coopérations et des solutions industrielles adaptées au marché visé.

Conclusion

Le logiciel de confiance, notamment dans les couches informatiques proches du matériel, doit être investi par les acteurs français et européens, c'est la clé nécessaire pour un retour possible vers le cœur des technologies de l'information et notamment vers la sécurité qui est un enjeu central pour la défense de la Nation. C'est à ce niveau que se joueront les marchés à venir et l'indépendance industrielle européenne dans des secteurs industriels critiques. Sur la base des efforts nationaux, des initiatives européennes doivent être prises dans un avenir prochain pour donner sa dynamique et sa place à cette question centrale. ☺



L'état du droit pénal

I/ L'accès frauduleux aux systèmes d'information

Le code pénal punit de deux ans d'emprisonnement et de 30 000 € d'amende l'accès frauduleux à un système de traitement automatisé de données. Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données, ou encore d'y introduire frauduleusement des données, est puni de cinq ans d'emprisonnement et de 75 000 € d'amende. Le fait, sans motif légitime, de détenir ou de fournir un équipement, un programme informatique ou toute donnée conçus ou spécialement adaptés à ces fins est puni des mêmes peines que l'infraction elle-même.

Le fait de détruire, détériorer ou détourner tout document, matériel, construction, équipement, installation, appareil, dispositif technique ou système de traitement automatisé d'informations ou d'y apporter des malfaçons, lorsque ce fait est de nature à porter atteinte aux intérêts fondamentaux de la nation, est puni de quinze ans de détention criminelle et de 225 000 € d'amende, voire de vingt ans de détention criminelle et de 300 000 € d'amende lorsque l'infraction est commise dans le but de servir les intérêts d'une puissance étrangère, d'une entreprise ou organisation étrangère ou sous contrôle étranger.

II/ La sécurité des données à caractère personnel

Selon la loi informatique et liberté et le code pénal, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende le fait de procéder à un traitement de données à caractère personnel sans prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

III/ L'atteinte au secret des correspondances

Le code pénal punit d'un an d'emprisonnement et de 45 000 € d'amende l'interception, le détournement et la divulgation des correspondances électroniques ainsi que l'installation d'appareils conçus pour réaliser de telles interceptions. De tels appareils doivent faire l'objet d'une autorisation de l'ANSSI pour être commercialisés ou détenus.

IV/ La cryptologie

Selon la loi du 21 juin 2004 pour la confiance dans l'économie numérique, l'utilisation des moyens de cryptologie est libre. La fourniture, l'importation et l'exportation des moyens de cryptologie assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont également libres. En revanche, la fourniture et l'importation d'un moyen de chiffrement sont soumises à déclaration préalable auprès de l'ANSSI qui peut demander à se faire communiquer les caractéristiques techniques du moyen de chiffrement ainsi que le code source des logiciels utilisés. L'exportation d'un tel moyen est soumise à autorisation de l'ANSSI. S'il a une vocation militaire, le moyen de cryptologie reste en tout état de cause soumis aux dispositions régissant les exportations de matériels de guerre. De manière similaire, la fourniture de prestations de cryptologie doit être déclarée auprès de l'ANSSI. Les infractions à la loi peuvent être constatées par des agents habilités à cet effet par le Premier ministre, par les officiers et agents de police judiciaire et par les agents des douanes.

La non-déclaration d'un moyen de cryptologie est punie d'un an d'emprisonnement et de 15 000 € d'amende. L'exportation en absence d'autorisation est punie de deux ans d'emprisonnement et de 30 000 € d'amende. Pour une entreprise, l'amende est quintuplée et diverses mesures pénales complémentaires peuvent être appliquées telle que l'interdiction d'exercer une ou plusieurs activités professionnelles ou sociales, la fermeture d'établissements ayant servi à commettre les faits incriminés, l'exclusion des marchés publics ou la confiscation de la chose qui a servi ou était destinée à commettre l'infraction.

En cas de confrontation des enquêteurs à des données chiffrées lors d'une enquête judiciaire, le code pénal prévoit la possibilité pour l'autorité judiciaire d'ordonner la mise au clair des données par toute personne physique ou morale qualifiée, voire par les moyens de l'État soumis au secret de la défense nationale si la peine encourue est égale ou supérieure à deux ans d'emprisonnement.

INEO DEFENSE

Votre partenaire dans les domaines de la Défense et de la Sécurité

UN SAVOIR-FAIRE COUVRANT LE CYCLE DE VIE DES SYSTEMES DEPUIS
LA RELEXION AMONT JUSQU'AU SERVICE OPERATIONNEL



UTILISATION
OPERATIONNELLE

REALISATION
DEPLOIEMENT

MAINTIEN EN CONDITION
OPERATIONNELLE

CONCEPTION

ETUDES AMONT (PEA, ETO)
ARCHITECTURE DE SYSTEMES



RETRAIT DU SERVICE
DEMANTELEMENT



DES METIERS MULTIPLES ET COMPLEMENTAIRES

CONCEPTION ET REALISATION DE SYSTEMES OPERATIONNELS

- d'information et de communications (SIOC)
- de recueil du Renseignement d'Origine Electro-Magnétique (ROEM) et de Guerre Electronique (GE)
- de détection, de surveillance et d'alerte - Homeland Security



INTEGRATION ET DEPLOIEMENT DE SYSTEMES MIS EN ŒUVRE EN ENVIRONNEMENT SEVERE (conditions NRBCE)

- dans des infrastructures fixes
- dans des structures mobiles, projetables et embarquables

REALISATION DES PRESTATIONS DE SERVICE ASSOCIEES

- ingénierie et management de la maintenance
- Maintien en Condition Opérationnelle (MCO)



INEO Défense

Zone Aéronautique Louis Bréguet
Route Militaire Nord – Bât 8
78140 VELIZY VILLACOUBLAY
www.ineo-defense-gdfsuez.com

Tél : 01 39 26 92 00

Fax : 01 39 26 92 02

Contact : sonia.vivet@ineo-gdfsuez.com

INEO
GDF SUEZ

Sécurité et confiance numériques

De la résilience des télécommunications à la sécurité numérique ou comment la révolution numérique bouscule nos critères de sécurité



par **Philippe Duluc**

Ingénieur en chef de l'Armement

Directeur de la sécurité groupe de France Télécom Orange

X82, ENSTA, après plusieurs postes au ministère de la défense dans le domaine du renseignement d'origine électromagnétique, il a conseillé le Secrétaire général de la défense nationale jusqu'en 2003. Il a été expert auprès de l'Agence européenne de la sécurité de l'information et des réseaux (ENISA). Il préside la Commission sécurité de la Fédération française des télécommunications, est membre du Conseil national de sécurité civile ainsi que du Comité de liaison défense du MEDEF.

La révolution internet nous ouvre sur le monde avec des services nouveaux partout. Elle nous met aussi à portée du moindre pirate informatique avec des menaces nouvelles. La stratégie de sécurité doit s'y adapter sans perdre de vue les principes fondamentaux.

On distingue généralement cinq critères de sécurité en ce qui concerne les ressources numériques :

- l'intégrité (elles ne peuvent être modifiées ou détruites que par un acte volontaire et légitime) ;
- la confidentialité (seules les personnes légitimement autorisées peuvent y accéder) ;
- la disponibilité (les ressources demeurent accessibles dans des conditions prédéfinies) ;

- l'imputabilité (on sait attribuer une action sur une ressource à un utilisateur déterminé) ;
- la non-répudiation (il est impossible pour son auteur de nier qu'une telle action ait bien eu lieu).

Tous les cinq sont fortement impactés par le développement du cyberspace.

Historiquement, la sécurité des télécommunications s'est surtout attachée

à la disponibilité des réseaux en particulier face aux incendies, aux pannes techniques et aux aléas climatiques (tempêtes, inondations). Les deux dernières catastrophes restent pour France Télécom l'incendie du central de Lyon-Sévigné en 1990 et les tempêtes de décembre 1999, deux événements ayant privé de téléphone plus d'un million d'abonnés chacun. Ces cas mis à part, les réseaux téléphoniques ont fini par devenir extrêmement résilients, en particulier grâce aux architectures

Des bons mots de passe tu choisiras

Pour ne pas être aisément retrouvé par un attaquant, un mot de passe doit être composé d'au moins 8 caractères (davantage s'il doit protéger des informations très sensibles), minuscules, majuscules, chiffres et caractères spéciaux et ne doit naturellement pas pouvoir être deviné. Il ne doit si possible pas être utilisé sur plusieurs services ou ressources distinctes, la compromission de l'un d'entre eux rendant vulnérables tous les services utilisant le même mot de passe.



STORM

Un botnet est un réseau d'ordinateurs (les zombies) commandés à distance par un pirate (le botmaster) à l'insu de leurs utilisateurs légitimes, à la suite d'une infection logicielle. On estime que fin 2007, Storm avait tenté d'infecter 1 à 50 millions de systèmes informatiques. Aujourd'hui en déclin, il aurait eu la capacité de réunir plus de 100 000 zombies simultanément. Plusieurs botnets ont été neutralisés ces dernières années : déconnexion en 2008 de McColo qui hébergeait les centres de contrôle de plusieurs botnets ; démantèlement du botnet Mega-D en 2009, de Waledac et de Mariposa plus récemment.

autocicatrisantes en anneau et à leur alimentation intégrée.

Mais le monde numérique se transforme du fait de la mondialisation et de l'ouverture à la concurrence, poussé par la réduction des coûts, le besoin de connectivité et de bande passante. Il est marqué par la convergence des besoins (fixe vers mobile, informatique vers télécommunications, voix vers données, civil vers militaire, etc.) et des technologies vers l'internet. Les communications électroniques se rapprochent du modèle économique de l'informatique de masse : développement ultrarapide, failles de sécurité détectées et corrigées tout au long du cycle de vie...

L'informatique industrielle en prend également le chemin, y compris les systèmes de supervision et de télégestion (SCADA, Supervisory Control And Data Acquisition) et peut-être demain l'informatique embarquée et l'informatique des objets. Cette révolution a des conséquences en termes de sécurité : l'interconnexion des réseaux facilite la propagation des virus et des vers informatiques ; avec l'informatique de masse, plus stratifiée, les mises à jour de sécurité sont plus difficiles ; le développement du cloud computing accroît les inquiétudes quant à la localisation des

données et donc sur leur confidentialité et leur disponibilité, comme en témoigne l'analyse de risques spécifique effectuée par l'Agence européenne de sécurité ENISA.

Trois grandes familles de menaces ciblent les ressources numériques

La première pointe les contenus (stockés ou transportés) portant atteinte à leur confidentialité ou à leur intégrité, comme :

- la collecte illégitime et massive de données personnelles sur internet (adresses mails, éléments bancaires, identités, mots de passe, etc.) à des fins d'escroquerie, de revente commerciale (pour de la publicité non sollicitée), voire de chantage à l'image ou la marque ;

- la recherche ciblée d'informations sensibles dans le domaine économique (concurrence) ou stratégique (États, organisations) ; subreptice, cette menace reste très difficile à détecter et à contrecarrer. Les autorités chinoises ont été notamment accusées, encore récemment, par plusieurs pays occidentaux de ce genre de pratiques.

La seconde concerne les contenants (systèmes, ressources d'information...) et porte atteinte à leur disponibilité ou

imputabilité :

- l'attaque reine, c'est le déni de service ; quand une ressource d'information est bombardée de toutes parts du réseau, elle n'est plus utilisable par personne ; c'est ainsi que les cybermanifestants ont procédé en Estonie en 2007 : louer un botnet -voir encadré- suffisamment puissant pour paralyser un site web pendant une journée ne coûte que quelques centaines de dollars sur internet. Le déni de service peut être généralisé et non ciblé comme ce le fut le cas avec le ver Slammer qui a saturé les réseaux en 2003 en moins de 15 minutes.

Enfin, la menace la plus difficile à parer est celle qui tire parti des faiblesses humaines, comme l'ingénierie sociale (qui exploite la psychologie des cibles : crédulité, crainte, confiance, compassion, etc.) ou l'hameçonnage (phishing) qui amène la victime à ouvrir des pièces jointes piégées ou à visiter un site web infecté : si des botnets géants se constituent, c'est principalement par manque de sensibilisation et de bon sens. Cette faiblesse peut aussi être culturelle ou liée à l'âge : si, étudiant, vous êtes immergé dans les réseaux sociaux et que vous vous exposez en mettant en ligne des



photos drolatiques de bizutage par exemple, vous le regretterez peut-être plus tard quand ces photos figureront dans votre dossier de recrutement chez un DRH.


Contre ces menaces nécessite de mettre en place une stratégie globale de sécurité qui se déploie en profondeur et qui responsabilise les utilisateurs

Sur les atteintes à la confidentialité et à l'imputabilité, il est de plus en plus difficile de tenir les pirates à distance des paquets de données traités. Le choix est cornélien : soit on cloisonne physiquement son réseau, ce qui peut être totalement incompatible avec les besoins des utilisateurs (interactions grandissantes avec l'extérieur), soit on s'ouvre physiquement à l'internet en filtrant les accès. Dès lors que l'on est relié à l'internet, une protection de bout en bout des informations sensibles paraît devoir s'imposer (chiffrement par l'expéditeur et déchiffrement par le seul destinataire légitime) ce qui nécessite de recourir à du chiffrement sans couture et à de l'authentification forte à base de certificats numériques. Le principal facteur humain à considérer ici est la tentation de sous-évaluer la sensibilité de ses propres données afin d'échapper aux contraintes :

il faut sensibiliser, responsabiliser et sanctionner. Cette approche de bout en bout apporte une garantie en matière d'intégrité : toute altération perturbe le processus de déchiffrement du message et se trouve donc immédiatement détectée. Elle ne permet en revanche pas d'assurer la disponibilité, qu'il faut traiter autrement.

Sur les atteintes à la disponibilité et à l'intégrité, il faut superviser dynamiquement la sécurité. D'abord, veiller les signes avant-coureurs, les signaux faibles provenant du microcosme des pirates, les parutions de failles et de correctifs, etc. Ensuite, qualifier la menace et prendre les mesures adaptées. Sur le plan opérationnel, il faut suivre en temps réel les paramètres techniques fournis par les équipements réseau et sécurité, détecter les anomalies et les analyser finement de manière à détecter les débuts d'attaque. Ensuite au plus fort d'une attaque (déni de service surtout) les principales mesures sont des mesures de compartimentage et de filtrage (blackholing) mais aussi d'adaptation dynamique du paramétrage des équipements réseau et sécurité : sur quelques cas réels, on a pu assister à de vrais duels entre botmaster et superviseur de sécurité, l'un modifiant les paramètres

d'attaque du botnet au fur et à mesure que l'autre les détecte et reconfigure les équipements réseau. Sur ces questions, il est crucial de disposer de capacités opérationnelles 24h/7j de veille et de supervision opérationnelle, fonction facilement mutualisable et qui gagne donc à être externalisée. Sur le plan humain, là encore, il s'agit de sensibiliser, de responsabiliser et de sanctionner, car une seule négligence humaine peut réduire à néant la stratégie décrite.

L'application des critères de sécurité évolue au même rythme que progresse la société de l'information. Plus les usages se répandent de façon mondialisée, plus la dématérialisation se met en place, plus les cybercriminels exploitent les vides juridiques existants, et plus la sécurité doit s'intégrer de façon globale et dynamique : équipements et applications spécifiques, mais aussi et de plus en plus sous forme de services, comme la supervision. La principale difficulté demeure le calcul du bilan économique qu'aujourd'hui seules les crises vécues permettent d'alimenter dans un mode strictement réactif et limité. 

ODAS



UNE SOCIÉTÉ DE L'ÉTAT FRANÇAIS ET DES INDUSTRIELS
DE DÉFENSE ET DE SÉCURITÉ



ODAS

339 Bureaux de la Colline
92213 - Saint-Cloud - France
T + 33 (0) 1 41 12 23 23
F + 33 (0) 1 41 12 22 97

Siso Co Ltd
PO Box 4720
Riyadh - 11412

Sécurité et confiance numériques

Les cartes bancaires et leur sécurité La version moderne du combat de l'obus et de la cuirasse

par **Pierre Juhen**

Ingénieur général des mines

Directeur Général de SER2S, filiale du Groupement des Cartes Bancaires "CB"

X-Télécom, Pierre Juhen a passé une grande partie de sa carrière au sein de France Télécom, où il a occupé des fonctions de R&D, de responsable de filiale, jusqu'à la direction d'un grand service de maîtrise d'œuvre de la Direction des Systèmes d'Information. En 2003, il rejoint le Groupement des Cartes Bancaires "CB" où il conduit le déploiement du nouveau réseau e-rsb, puis le processus de filialisation de l'activité.

La carte bancaire est devenue le moyen de paiement préféré des Français. En 1997, le nombre de paiements par chèque était deux fois supérieur à celui des paiements par carte. En 2009, la proportion s'est inversée. Ce moyen de paiement universel attire évidemment les fraudeurs du monde entier, qui profitent des vulnérabilités du système, que les banquiers renforcent en permanence.

La carte bancaire est devenue le moyen de paiement préféré des Français. En 1997, le nombre de paiements par chèque était deux fois supérieur à celui des paiements par carte. En 2009, la proportion s'est inversée.

Derrière le geste simple qui consiste à introduire sa carte dans un terminal et composer ensuite son code secret se trouvent une organisation et une infrastructure complexes, qui permettent de débiter le compte du client et de créditer le compte du commerçant dans des conditions de rapidité et de sécurité optimales.

Principes de fonctionnement d'un système de paiement par cartes

La caractéristique d'un paiement par carte est qu'il est garanti pour le commerçant, lorsqu'il y a utilisation de la puce et frappe

du code secret. C'est la banque du titulaire de la carte qui apporte sa garantie à sa consœur, qui ensuite garantit le commerçant.

Pour gérer le risque associé, la banque doit pouvoir gérer l'encours du titulaire de la carte en temps réel. C'est pourquoi un acte de paiement fait l'objet d'une demande d'autorisation dès lors qu'il dépasse un certain montant, variable selon le contrat établi entre la banque et son client.

Entre les banques, cette demande d'autorisation est acheminée via le réseau e-rsb. (Voir encart)

À la fin de la journée, les transactions sont collectées par la banque du commerçants, et échangées sur la plate-forme de compensation, ce qui permet leur règlement.

La fraude et sa prévention

Comme tous les moyens de paiement, la carte bancaire est l'objet d'attentions de la part des fraudeurs.

Historiquement, la fraude la plus importante est liée à l'utilisation de la piste magnétique, qu'il est maintenant facile de copier. Dès les années 80, les banques françaises ont décidé de déployer la carte à puce pour parer cette faiblesse, suivies par les banques européennes dans les années récentes. Ceci a permis de réduire ce type de fraude de manière considérable. Néanmoins, de nombreux pays, dont les États-Unis, n'ont pas encore décidé de migrer vers la technologie "Chip and Pin". Les fraudeurs peuvent donc utiliser les données volées en Europe, pour forger de fausses cartes, qu'ils peuvent utiliser dans des commerces, voire dans des distributeurs de billets, s'ils ont pu

Les cookies tu supprimeras pour conserver l'intimité de ta navigation

Les cookies, petits fichiers placés sur l'ordinateur par les sites consultés, permettent aux responsables des sites et aux prestataires de publicité, tels que Google, de connaître de nombreux détails sur votre navigation et vos thèmes d'intérêt ; il peut être bon de les supprimer de temps en temps, voire de les interdire pour certains prestataires que vous considérez comme intrusifs.



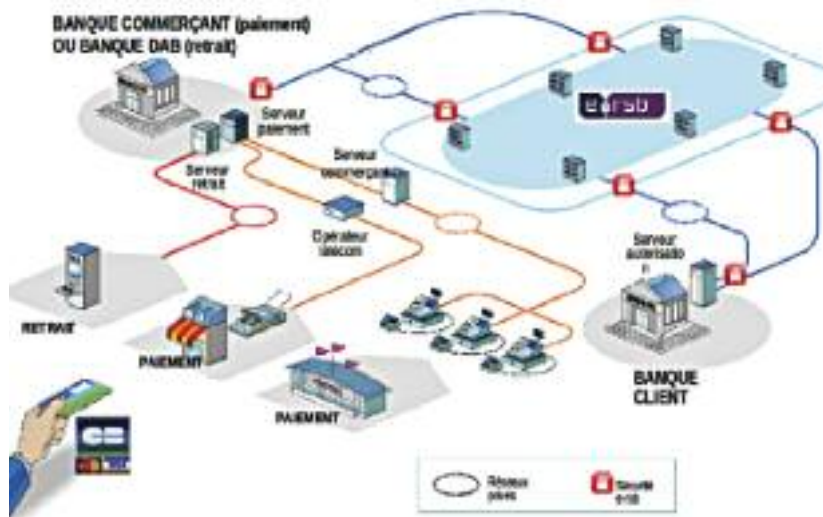
également accéder au code secret, avec une micro-caméra, par exemple.

Au cours des années 2000, une fraude connue sous le nom de "YesCard", a affecté les cartes à puces françaises, d'ancienne technologie (BO'). Le déploiement de nouvelles cartes de technologie EMV/DDA a complètement jugulé cette vulnérabilité.

Mais la fraude la plus préoccupante aujourd'hui concerne l'utilisation de la carte pour le paiement sur Internet. La carte bancaire était en 2000, et demeure, le seul instrument qui permette un paiement à distance instantané. L'explosion du e-commerce s'est accompagnée d'une fraude qui est maintenant la plus importante.

Conscient du danger, les systèmes de paiement ont conçu un mode de fonctionnement dédié à Internet, appelé "3D-Secure" qui permet à chaque banque de vérifier l'identité du porteur de la carte au moment de la transaction, en choisissant le mode de vérification. C'est ainsi que certaines offrent à leurs clients une "calculatrice" dans laquelle vient se glisser la carte à puce, d'autres leurs envoient un code par SMS, certaines posent une question secrète. Mais ce système ne concerne à l'heure actuelle que moins de 20% des transactions de vente à distance.

Alors, face à ces menaces, faut-il avoir peur d'utiliser sa carte, sur Internet en particulier ? Non, car la loi est très protectrice pour le consommateur, et les victimes de fraude sont remboursées par leurs banques, qui elles, assument le coût de cette fraude. C'est pourquoi elles continuent d'investir pour renforcer la sécurité de ce moyen de paiement, qui est aujourd'hui le plus universel, tant par sa couverture géographique que la diversité de ses modes d'utilisation.



e-rsb

Le réseau e-rsb est le système qui relie les banques entre elles, et route les demandes d'autorisations. C'est un système qui doit fonctionner 24 heures sur 24, 7 jours sur 7, avec une disponibilité contractuelle de 99,999% (soit moins de 5 minutes par an d'indisponibilité). Sa redondance permet d'assurer la résilience attendue, et d'assurer sa maintenance sans jamais interrompre le service.

Dès qu'un terminal demande une autorisation, il l'envoie vers la banque du commerçant, qui la signe, et la poste sur e-rsb. Celui-ci vérifie la signature, calcule les destinations possibles (à partir des premiers numéros de la carte, qui détermine la banque de manière unique) re-signe le message et l'envoie vers son destinataire.

La réponse est acheminée selon le chemin inverse; le temps total de traitement est de l'ordre de 0,4 secondes, le serveur de

la banque destinataire calculant la réponse en environ 0,35s et le réseau conduisant ses opérations en 0,05 secondes environ. e-rsb traite actuellement 450 demandes d'autorisation par secondes en pointe et 3,4 milliards de demandes par an, mais pourrait en acheminer beaucoup plus. Conçu au début des années 2000 avec CS Communication et Systèmes, il est en cours de refonte pour tenir compte des évolutions technologiques et surtout lui permettre d'offrir son service non seulement en France, mais également en Europe.

En effet, le monde des moyens de paiement, jusqu'à présent très domestique, évolue sous l'impulsion de l'Union Européenne, vers une unification. C'est pourquoi la Direction Informatique et Réseaux du Groupement des Cartes Bancaires CB est devenue, depuis le 1er janvier 2010, la Société d'Exploitation de Réseaux et de Services Sécurisés (SER2S), pour répondre à ce nouvel enjeu. 📡

Sécurité et confiance numériques



Les mêmes précautions sur ton smartphone tu prendras

Les téléphones intelligents sont de véritables ordinateurs, souvent moins bien protégés que les ordinateurs personnels. Par exemple, il n'est pas toujours possible de naviguer sans être administrateur ni de mettre à jour les logiciels. Les recommandations précédentes doivent donc, à chaque fois que possible, être suivies avec d'autant plus de soin.

Internet et ses ruptures ?

par **Arnaud Salomon**

A l'image de la machine à vapeur ou de l'électricité, leviers d'une Révolution industrielle ? De l'imprimerie, levier d'une Renaissance ? Du passage des hiéroglyphes Egyptiens, élitistes et finalement abandonnés, aux écritures plus partagées, et en premier lieu, dans la période antique, la Grecque ? du passage à une nouvelle Histoire ?

Quoi qu'il en soit, l'Internet, et plus largement les systèmes d'information, sont bien là, avec leur cortège de fonctions, d'applications, de bases de données, pour le meilleur comme pour le pire ; comme la langue elle-même, depuis Esope, comme la technologie !

Nos infrastructures vitales, énergie, télécommunication, administrations, reposent sur des systèmes d'information et communication, dès lors eux-mêmes vitaux.

La compétitivité de presque toutes nos activités, ou seulement même leur possibilité, repose sur des systèmes d'information collectant de plus en plus d'informations individuelles : dossiers médicaux, fichiers de Police, fichiers bancaires, fichiers éducatifs...

Big Brother, projeté en "1984" dès 1948 par Orwell, peut se mettre à l'œuvre.

Identification de toutes les liaisons numériques et de leur contenu (courrier, voix, données), de tous les liens entre personnes.

Identification de tous les paiements numériques, en conséquence de tous les actes associés de la vie privée, de leurs dates, heures et localisation.

Géolocalisation au travers des cartes d'abonnement de transport, des cartes de péage numérique, des récepteurs de radionavigation.

Vidéo surveillance généralisée, permettant de voir qui est où quand, avec qui...

Bien sûr, "qui n'a rien à se reprocher n'a rien à craindre" ! Tout comme il est le détenteur de la violence légitime, l'Etat, ou ses délégués, peuvent bien être les détenteurs

d'information sur la vie privée.

Mais ces systèmes d'information sont-ils si sûrs ? On les sécurise, on s'assure qu'ils ne sont pas détournés. Et on punit les coupables, s'ils sont pris et s'ils peuvent en effet tomber sous le coup de nos lois... qui n'ont pas, chacun le sait bien, de portée universelle.

Qui garantit, et ce de manière certaine, qu'une puissance mal intentionnée ne peut pas détourner ces informations pour en faire usage à son profit, ou, plus sournoisement encore, les modifier, les polluer.

Un des grands secrets les mieux gardés fut qu'Enigma avait été cassée.

Lesquels de nos systèmes d'information sont ou ne sont pas cassés ou cassables ? ☹



Une approche globale de la cyber sécurité

par EADS Solutions & Services

Omniprésents, les réseaux de communication font désormais partie de notre vie quotidienne. Plus flexibles, ils deviennent aussi plus fragiles face aux incidents ou aux attaques, provoquant des interruptions de service et induisant d'importants coûts de remise en état.

Afin de s'adapter, la sécurité des systèmes d'information doit franchir un palier et s'abstraire des couches technologiques basses pour venir s'intégrer tout au long de la chaîne de traitement de l'information, utilisateurs, techniciens et décideurs. Il faut donc une vision globale qui s'appuie sur trois composantes indissociables : des technologies de pointe, des processus opérationnels formalisés, régulièrement exercés, et des ressources humaines efficacement formées et entraînées.

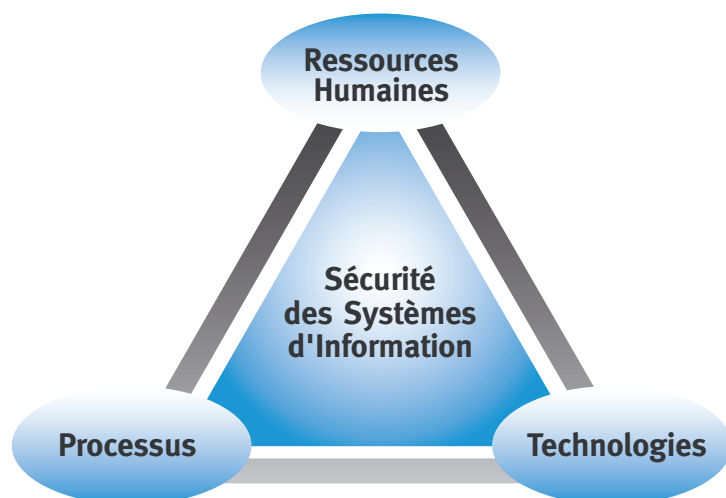
Ce triptyque garantit une gestion de la sécurité des systèmes d'information adaptée à l'organisation et à ses acteurs. Les décideurs, par exemple, doivent recevoir les éléments de bon niveau pour planifier un engagement financier et organisationnel cohérent dans la durée et, en cas de crise, disposer de l'information pertinente en temps réel. Pour les techniciens, c'est la garantie d'une structure efficace, bien dimensionnée, et dont les succès sont mesurables.

Cette approche guide toute la démarche de développement et d'intégration d'EADS Defence&Security (DS) pour ses solutions de gestion de la sécurité des systèmes d'information. Tout d'abord, la formation des opérateurs, la conduite d'exercices et la simulation deviennent des activités centrales. EADS DS propose HOTSIM® et CYNTRS® utilisés par l'US Air Force pour former et entraîner ses opérateurs. Ces simulateurs ont également contribué à des exercices majeurs tels que CyberStorm piloté par le DHS américain.

Ensuite, le Cockpit de Sécurité forme le cœur de la supervision de la sécurité. Intégré au-dessus des capteurs et des sondes, il abstrait la complexité technologique pour se concentrer sur la juste réaction aux incidents. Grâce à ce système, l'opérateur n'a d'ailleurs plus besoin d'être un expert technique.

Enfin, EADS DS a mis en place une cellule de maintien en condition de sécurité (MCS) au service de ses projets, en liaison constante avec les équipes de maintien en condition opérationnelle (MCO), pour une prise en compte optimale des mises à jour de sécurité.

Finalement, avec cet équilibre, la sécurité des systèmes d'information est mieux gérée et mieux prise en compte à tous les niveaux. Elle est plus performante, tout simplement.





Alcatel-Lucent

Les réseaux de communications

au cœur de la sécurité des systèmes d'information et de la confiance numérique

Parmi les moyens mis en œuvre pour assurer la sécurité des systèmes d'information (SSI), les réseaux de communications tiennent une place prépondérante. Toutefois, les nouvelles technologies Internet et la convergence IP permettent-elles de bâtir des réseaux de communication totalement sécurisés et d'assurer une parfaite intégrité et confidentialité des informations ?



Jean-Marc.Pezeret@alcatel-lucent.com

Nous avons interrogé Jean-Marc Pézeret, directeur en charge du Ministère de la Défense chez Alcatel-Lucent France, de façon à connaître le point de vue du leader des réseaux haut débit fixes, mobiles et convergés, des technologies IP et services.

Mr Pézeret, de par votre expérience dans le domaine des réseaux de communications critiques, quelles sont les principales tendances que vous observez dans l'expression des besoins du ministère de la Défense ?

Trois grandes tendances sont à noter: le recentrage des opérationnels sur leur cœur de métier militaire, la réduction des coûts opérationnels, de maintenance et de communications ; et enfin la pérennité des investissements et des technologies. Le tout sans compromis sur la fiabilité et la sécurité autre que l'abandon des spécificités non standards.

Justement, est-il concevable de répondre à l'ensemble de ces objectifs apparemment contradictoires ?

Rien ne s'y oppose, bien au contraire. Les

nouvelles technologies IP de type MPLS¹ et SIP² permettent de concevoir des réseaux convergents de haute fiabilité tout en assurant une migration en douceur des réseaux existants (TDM, ATM,...). Les qualités et niveaux de service sont garantis de bout en bout, et donc compatibles avec les exigences des réseaux critiques.

Des produits et solutions standards issus du monde civil permettent de réduire les coûts d'acquisition et de maintenance. Des réseaux entièrement convergés (voix, données, vidéo) réduisent les coûts de gestion et de communication. Enfin, les standards Internet et "open source" sont gages de grande fiabilité et sécurité. La preuve : nos solutions de téléphonie IP/SIP sur système Linux sont certifiées ISO15408 (Critère Commun) par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Nos commutateurs Ethernet sont conformes aux standards militaires MIL-STD.

Quels clients utilisent ces technologies standards dans des réseaux critiques ?

Les exemples sont nombreux. Je citerai dans le domaine du transport :

- La société ferroviaire suédoise Banverket qui a choisi de déployer un réseau IP/MPLS pour toutes ses communications, y compris celles relatives à ses missions les plus sensibles comme la signalisation.

- Son équivalent en Norvège, la société Jernbaneverket qui a également associé ses communications mobiles opérationnelles GSM-R.

- et en Angleterre, UK Highways Agency, qui a migré son réseau vers un réseau IP unifié plus fiable et plus économique.

Autre exemple, dans le secteur de l'énergie;

- RTE, le gestionnaire du réseau de transport d'électricité français, a déployé et sous-traité l'exploitation d'un réseau haut débit entièrement optique pour les communications



stratégiques de son infrastructure de transport d'électricité haute tension ainsi que pour son réseau de sécurité ROSE.

Enfin dans le domaine de la sécurité publique; - les autorités et organisation de sécurité allemandes (BDBOS - Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben) ont sous-traité à Alcatel-Lucent l'exploitation et les évolutions du plus grand système de communication radio numérique TETRA³ au monde avec 500 000 utilisateurs. Ce réseau permet de garantir les communications entre les différentes organisations de sécurité et de secours (police, services médicaux, pompiers...) au quotidien et en situation de crise et d'urgence.

Ces sociétés aux activités très sensibles n'hésitent plus à faire le choix des nouvelles technologies et également à adopter de nouveaux modèles économiques de sous-traitance ou de cogérance. Comment expliquez-vous ces changements ?

Deux facteurs motivent ces changements. Tout d'abord la volonté de ces sociétés de se recentrer sur leur cœur de métier, d'agir en tant que donneur d'ordres et de laisser aux spécialistes la complexité des technologies. Ensuite, le souhait de bénéficier de l'expérience des autres sur des

problématiques similaires, telles que la sécurité des réseaux IP et de l'information. A titre d'exemple, nous mettons à disposition de nos clients nos expertises et compétences, avec notamment notre représentation active au sein du CERT-IST⁴. Nous proposons également des centres opérationnels de sécurité⁵ pour gérer en partenariat avec les équipes sécurité de nos clients les politiques sécuritaires de manière proactive ainsi que les plans de continuité d'activité et de gestion de crises.

Quelles seraient vos recommandations pour démarrer un projet de transformation d'un réseau vers l'IP avec un niveau d'exigences maximal en matière de sécurité et de fiabilité ?

Tout d'abord, il convient de parfaitement connaître l'existant en termes de niveaux de services fonctionnels, opérationnels et de contraintes sécuritaires. Puis, de définir une architecture cible qui tienne compte des évolutions technologiques, de la pérennité de ces technologies, de l'évolution des standards et surtout de l'évolution des besoins de bande passante, des types de trafic, des besoins fonctionnels et opérationnels.

Concevoir cette nouvelle architecture cible à travers un modèle de sécurité éprouvé :

ITU/T X.805 et ISO18028, initialement inventé par Bell Labs, le laboratoire d'innovation d'Alcatel-Lucent. Il est maintenant normalisé. Définir enfin les étapes pour passer de l'existant à l'architecture cible. Nous mettons à disposition nos compétences pour auditer, concevoir et implémenter ce type de réseaux IP de nouvelle génération hautement sécurisés.

Merci de nous avoir éclairés sur la transformation des réseaux, au cœur du dispositif de sécurité des systèmes d'information.

¹ Internet Protocol / MultiProtocol Label Switching - La majorité des grands opérateurs utilisent aujourd'hui MPLS dans la partie centrale de leur réseau pour assurer l'ingénierie de trafic et la qualité de service.

² Session Initiation Protocol (SIP) est un protocole standard ouvert de gestion de sessions souvent utilisé dans les télécommunications multimédia (son, image, etc.). Il est depuis 2007 le plus courant pour la téléphonie par internet (la VoIP).

³ Terrestrial Trunked RAdio - norme ETSI (European Telecommunications Standard Institute) EN 300 392 pour les systèmes de radio mobile numérique professionnels.

⁴ Computer Emergency Response Team, le CERT dédié à la communauté Industrie, Services et Tertiaire française

⁵ SOC - Security Operation Center

Continental



Partenaire privilégié de la défense

Le marché des blindés à roues a fortement progressé depuis la fin des années 80 suite à la chute du bloc communiste. Les conflits conventionnels imaginés entre les 2 super puissances étaient composés de vagues de blindés lourds, donc chenillés, hors agglomération (les belligérants auraient évité les combats en ville suite aux leçons de la bataille de Stalingrad pendant la 2^{ème} Guerre Mondiale). La fin de la menace d'un

conflit entre armées puissantes, et l'apparition de conflits de type guérilla de basse ou de moyenne intensité, nombreux et lointains, ont mis les blindés à roues au premier plan. Plus facilement projetables que leurs homologues chenillés car nettement moins lourds, ils sont mieux adaptés à la guerre urbaine grâce à leur faible encombrement. Ils sont aussi plus rapides et moins gourmands en carburant simplifiant ainsi la logistique.

Churchill disait d'ailleurs en parlant de la logistique militaire que "la guerre était une opération de transport et que le meilleur transporteur en sortirait vainqueur". Cette citation prend évidemment tout son sens dans les conflits d'aujourd'hui où la capacité de projection et de soutien (soutien pétrolier et de l'homme, appui à la mobilité des blindés moyens et lourds) est devenue plus que jamais primordiale si une armée désire rester efficace.

C'est dans ce contexte qu'intervient, depuis plus de 30 ans, le Groupe Continental en fournissant aux Armées Françaises et Etrangères, mais aussi aux constructeurs de véhicules militaires, des solutions dans le domaine des pneumatiques tout-terrain. Continental conçoit, développe et fabrique une large gamme de pneumatiques Off Road afin de répondre aux besoins en mobilité exprimés par les unités opérationnelles, principales utilisatrices de nos pneumatiques.

Le Groupe Continental est présent à la fois sur le marché de la première monte chez les principaux constructeurs de véhicules militaires, mais également sur le marché du remplacement où il est devenu, au cours de ces trois dernières décennies, le principal fournisseur de l'Armée de Terre Française en pneumatiques. Continental équipe aujourd'hui tous les types d'engins en service dans les Armées qu'ils soient logistiques ou tactiques. Ce ne sont pas moins de 18 000 véhicules militaires qui roulent tous les jours sur des pneumatiques conçus et fabriqués par le groupe Continental, et cela sur tous les théâtres d'opérations. Continental fournit, en remplacement ou en première monte, des



CAESAR équipé en 365/80R20 MPT 81



GBC 180 équipé en 13R22,5 HSO

pneumatiques pour les porteurs à plateau déposable **VTL**, pour les véhicules cargo tous terrains **GBC180 6x6**, pour les poids lourds de transport militaire **TMR10000 6x6**, mais également pour le véhicule de transport de troupes blindé **VAB**, le camion équipé d'un système d'artillerie **CAESAR** ou le dernier camion citerne **R114CB 6x6 HZ340 CCP10** etc...

Le Groupe Continental a gagné plusieurs marchés militaires dans le cadre de vastes programmes de rénovation de véhicules militaires comme celui concernant la déconstruction complète du légendaire **GBC 8KT**, devenu aujourd'hui le **GBC180** ou celui concernant le **VAB**. La société a fourni au travers de ces deux programmes, deux pneumatiques poids lourds répondant parfaitement aux exigences qu'attendent les militaires d'un pneumatique Off Road c'est à dire : mobilité, efficacité sur tous les terrains et maîtrise des coûts. Ces deux pneumatiques poids lourd sont le **13R22.5 149/146J HSO Military Continental** et le **14.00R20 160/157G T9F Uniroyal'** dont l'excellent rapport/qualité prix n'est plus à démontrer. Ils équipent respectivement aujourd'hui le **GBC180** et le **VAB**.

Le pneumatique poids lourd **13R22,5 HSO Military** possède en effet, de fortes capacités de mobilité grâce à la géométrie et à la structure du dessin de la bande de roulement. Il bénéficie d'une carcasse renforcée haute longévité même soumise à des charges extrêmes. Ces mélanges de gomme innovants limitent l'impact des blessures lui assurant une durée de vie maximale en tout-terrain. Le **13R22,5 HSO Military** est donc un pneu à la fois robuste, endurant et efficace tout en restant économiquement compétitif. Dans ces conditions, il est facilement compréhensible de le retrouver également en première monte sur des véhicules militaires Renault trucks Défense de la gamme **Sherpa 2** ou **3** ; véhicules actuellement en service à l'OTAN ; ou le **Sherpa 5 euro 2**.

La nouvelle génération de profils Continental tout-terrain **HCS** pour pneumatiques poids-lourds est arrivée. Ce nouveau profil vient compléter la gamme dans les dimensions : **365/85R20 164J TL**, **395/85R20 168J TL** et **14.00R20 164/160J (166/160G) TL** et propose une solution -aux usages mixtes des véhicules (route/tout-terrain) très éprouvants

pour les pneumatiques- à profil 100% Off Road. Sans rien sacrifier, le profil **HCS** réussit le tour de force de conserver de bonnes capacités de mobilité tout en ayant un excellent comportement routier. Allié à de nouveaux mélanges de gomme à faible résistance au roulement, le profil **HCS** assure sur route confort et sécurité, rendement kilométrique élevé et économie de carburant. Le Groupe Continental innove donc sans cesse en proposant des solutions dans le domaine des pneumatiques tout terrain et participe à la maîtrise des coûts d'exploitation et à la préservation de l'environnement. Le **395/85R20 168J HCS Continental** équipe actuellement une grande partie du parc de véhicules d'incendies de piste de type **SIDES VMA 4x4** ou **6x6** en service sur les bases aériennes de l'Armée de l'Air Française. Soumis en permanence, dans cette mission, à des charges importantes et des accélérations fortes, le pneu poids lourd **395/85R20 HCS Continental** offre d'excellentes performances en toutes circonstances.

Créé en 1871 à Hanovre le Groupe Continental AG est présent aujourd'hui dans 46 pays sur



quelques 190 sites et emploie environ 138 000 personnes réparties dans 2 divisions : la division Automotive (automobile) et la division Rubber (caoutchouc). Avec la division Automotive, le Groupe Continental est aujourd'hui le 5ème équipementier Mondial (2ème Européen), le numéro 1 mondial des systèmes de freinage (disques, plaquettes, étriers) et le numéro 2 mondial des systèmes des freinages électronique (ABS et ESP). Dans la division Rubber, Contitech est le numéro 1 mondial des pièces techniques caoutchouc et polymères. Avec un investissement en R&D représentant 4,5% de son chiffre d'affaire et plus de 18 000 ingénieurs, le groupe Continental dépose plus de 1000 brevets par an. Enfin le département pneumatique conçoit et fabrique des pneumatiques destinés à tous les véhicules terrestres. Chaque année, le groupe Continental AG produit à travers le monde plus de 100 millions de pneumatiques Tourisme, près de 7 millions de pneumatiques Poids-lourd et plus de 600 000 pneumatiques Industrie. Continental est le numéro 1 des ventes de pneumatiques tourisme en Europe (équipements d'origine et remplacement) - en France 1 véhicule sur 3 est équipé d'origine en pneus Continental.

Partenaire global de l'industrie automobile, Continental concentre ses compétences sur le châssis et la liaison au sol. Manufacturier de pneus, fournisseur de systèmes et centre d'ingénierie, Continental collabore avec tous les constructeurs pour améliorer sans cesse le confort et la sécurité des véhicules. De manufacturier au statut de leader mondial de la liaison au sol, le groupe Continental est présent sur 100% des véhicules fabriqués en Europe !

La marque Uniroyal est une marque du Groupe Continental AG

Jean-Marc Veaux
Responsable Comptes Clés Administrations/Défense
jean-marc.veaux@conti.de

www.continental-corporation.com



Continental HCS



Continental HSO Military

Avec un chiffre d'affaires d'environ 20Mrd d'euros en 2009, le Groupe Continental fait partie des premiers fournisseurs automobiles dans le monde. En tant que fournisseur de systèmes de freinage, de systèmes et de pièces pour moteur et châssis, d'instrumentations, de solutions multimédia embarquées, d'électronique automobile, de pneus et d'élastomères, l'entreprise contribue à une plus grande sécurité de conduite et à une meilleure protection de l'environnement. En outre, Continental est un partenaire compétent dans la communication automobile intégrée. L'entreprise emploie actuellement environ 138 000 collaborateurs répartis dans 46 pays.



“DÉFENSE ET SÛRETÉ DANS LE VAR” une filière d'excellence

Le secteur économique lié à la défense et à la sûreté dans le Var est remarquable. Le département concentre tous les acteurs civils et militaires. Au côté de grands groupes, le tissu de PME réunit, en matière de développement de technologies de pointe, des savoir-faire et spécificités reconnus à l'échelle internationale. Les grands projets d'innovation, auxquels sont associés l'ensemble des entreprises varoises, sont une marque de l'excellence des produits et services qu'elles présentent.

Défense dans le Var : une légitimité historique

- 1^{er} département militaire, historiquement tourné vers la marine et l'aéronautique navale.
- Toulon, base historique de la Marine française en Méditerranée depuis le XVI^e siècle. 1^{er} port militaire européen et 1^{er} base navale de défense en Méditerranée.
- Toulon, port d'attache du porte-avion nucléaire et des six sous-marins nucléaires d'attaque.
- 6 sites militaires complémentaires : L'Atelier Industriel de l'Aéronautique de Cuers-Pierrefeu (AIA CP) - Cauijers, le plus grand camp d'entraînement d'Europe - Le CIN de Saint-Mandrier, plus grand centre d'instruction de la Marine Nationale - L'École d'Application de l'Artillerie de Draguignan (EAA) - L'École d'Application de l'Aviation Légère de l'Armée de Terre au Luc (EAALAT) - L'École Franco-Allemande Tigr au Cannet-des-Maurs.

Le Var : une réponse aux besoins des industries militaires et civiles

- Très forte concentration des cultures locales historiques - Armée de Terre - Marine Nationale
- Très fort impact des activités industrielles et services liés à la défense et à la sûreté.

Délégation Générale pour l'Armement - DGA

- CELM - Essais de lancement de missiles - Toulon et Ile du Levant
- CTSN - Systèmes navals - Sécurité aux rayonnements électromagnétiques - Toulon

Le Var : position stratégique au cœur de l'innovation et des pôles de compétitivité

- Pôle Mar PACA, Pôle OPTITEC, Pôle Pégase et Pôle Solutions Communicantes Sécurisées.
- Toulon Var Technologies entretient depuis 20 ans des liens étroits avec le monde de la Défense.

La région PACA, un environnement riche

Des formations adaptées aux besoins du secteur : La région compte 10 écoles d'ingénieurs, 16 IUT, 3 formations de pilote avec l'EPNER, EAALAT, École de l'Air et le CIN de Saint-Mandrier (Centre d'Instruction Navale).

Grands donneurs d'ordre :

CNIM (Var), DCNS (Var), EUROCOPTER, GROUPE DASSAULT, SNECMA MOTEURS, TECHNICATOME, THALES ALENIA SPACE, THALES UNDERWATER SYSTEMS.

Chiffres clés :

- Près de 200 PME de sous-traitance, 2 500 emplois en R&D privée.
- Près de 30 000 emplois civils et 45 000 emplois militaires.
- 8 centres d'essais dédiés aux domaines aéronautique et spatial.
- Plus de 12 laboratoires de recherche publique en aéronautique spatiale défense - 3 000 chercheurs.
- 13 centres de R&D spécialisés en optique, mécanique, matériaux et énergétique, 700 chercheurs publics.

Le Var : carrefour des échanges mondiaux en Méditerranée

- Au cœur de la 3^e région économique française Provence-Alpes-Côte d'Azur (PACA).
- Au carrefour des axes Espagne-Italie et Europe du Nord-Méditerranée.
- Au centre des pôles économiques majeurs : Marseille, Nice, Lyon, Barcelone, Milan.
- À proximité des marchés de l'Europe de l'Est.

VAR ACCUEIL INVESTISSEURS

L'agence de développement économique née de la volonté du Conseil Général du Var et de la Chambre de Commerce et d'Industrie du Var.

Favorise et accompagne l'implantation des investisseurs dans le Var :

- Accueil des dirigeants d'entreprises
- Analyse conjointe des projets
- Aide à la recherche de terrains et locaux
- Suivi dans l'ingénierie du projet
- Mise en relation avec les partenaires économiques, financiers et institutionnels du département.

Contact Var Accueil Investisseurs :
04 94 22 80 68 - vai@var.cci.fr



Trois présidents, un visage

par **Michel Clamen**

La présidence suédoise a accompli un travail considérable et, malgré le retentissement négatif du sommet de Copenhague, chacun la considère comme un succès. Le nombre des textes adoptés a pu occulter le plus important pour l'Armement : perdue dans la masse, la directive sur les marchés de défense nous concerne directement (voir encadré).

L'Espagne a pris le relais, puis viendra la Belgique. Présidences de crise, décidées à jouer une stratégie de redressement : faire face aux urgences financières favoriser croissance et emploi, prolongeant ainsi la "stratégie de Lisbonne"; maintenir, malgré le semi-échec de Copenhague, l'avance européenne dans l'ère post-Tokyo; mettre en place la politique énergétique face à la Russie; reformer la PAC... un tel agenda ressemble déjà une gageure.

Viennent s'y ajouter les péripéties d'une réforme institutionnelle, puisque cette année 2010 est celle où entre en vigueur une novation de première grandeur, concrétisée par deux postes nouveaux. Rappelons qu'un Président permanent du Conseil européen a désormais pour vocation d'animer les 27 chefs d'État dans leur rôle d'orientation politique, ce qui ne se confond pas avec la présidence tournante du Conseil des ministres, seule assemblée co-législatrice : au Président les grands choix, à la présidence tournante la mise au point juridique des textes. Le poste est dévolu à Herman van Rompuy, belge.

De plus, un Haut représentant, qualifié souvent de "Ministre des affaires étrangères" de l'Union, incarne cette dernière dans ses relations avec le reste du monde. Ce poste est dévolu à Mme

Ashton, britannique. A elles deux, ces personnalités vont donner un visage à l'UE, de quoi répondre post mortem au persiflage de Kissinger : "l'Europe, quel numéro de téléphone ?"

Ces nominations n'ont pas rencontré tout de suite l'unanimité. Comme toujours en Europe, il a fallu un compromis, qui ne se situe pas forcément à l'optimum : si le savoir faire de H. van Rompuy apparaît déjà, sa collègue semble pour l'instant moins charismatique. Il faut y voir le fruit de la décision collective - "un chameau est un cheval dessiné par un comité".

L'arrivée de ces deux personnalités, qui viennent se surajouter à l'existant, marque un changement profond, et pas seulement pour le Conseil lui-même. Car pour la Commission, habituée à un Président qui n'est là que pour 6 mois, la permanence

Du nouveau sur les marchés publics

Depuis aout dernier, les États-membres ont deux ans pour transposer en droit national la directive sur les procédures de passation de marchés dans les domaines de la défense et de la sécurité.

Les dispositions essentielles en sont les suivantes : la "procédure négociée avec publication d'un avis de marché" s'applique sans restrictions; les questions de sécurité d'approvisionnement et de sécurité de l'information font l'objet de mesures spécifiques; il en est de même pour la sous-traitance, les voies de recours; des exclusions sectorielles sont prévues. De ces dispositions "sur mesure" il est attendu une transparence et une efficacité accrues. Comme souvent, l'adaptation aux réalités du terrain sera plus ou moins réussie suivant ce que fera chaque État-membre.

La Commission, quant à elle, considère qu'avec ce texte, le marché européen des équipements de défense devient une réalité.

au Conseil européen change complètement les perspectives. Et comment vont se distribuer les rôles entre le Président du Conseil européen et la présidence tournante du Conseil des Ministres ?

A nouveaux postes, nouveaux acteurs. Si éminents qu'ils soient de part et d'autre, et en raison même de leurs fortes personnalités, la question de bonne coordination se pose. Hermann Van Rompuy, José Manuel Barroso et le Président (tournant) du Conseil des Ministres auront fort à faire pour trouver un équilibre.

Les premiers temps de fonctionnement dans la géométrie nouvelle sont en train de créer l'usage.

Dès février, le premier sommet européen

a marqué un changement de régime. Rencontre économique, mais surtout réunion au secours de la Grèce. C'est Herman van Rompuy qui a porté la parole, première réponse de l'UE par laquelle elle a fait connaître sa solidarité morale, dans l'esprit sinon dans les actes. Même si la défiance des marchés n'en a pas été dissipée, l'intervention (renforcée depuis par celle de fin mars) a traduit un symbole, celui de la distribution nouvelle des rôles à laquelle on peut s'attendre. C'est à Bruxelles que se créait l'évènement et non avec l'intronisation de la Commission Barroso.

Ce nouvel ordre européen, marqué par un certain effacement de la Commission, signifie-t-il le déclin du projet européen ? Non, simplement, à partir d'aujourd'hui s'ouvrent de nouvelles routes institutionnelles. Un président de la

Commission, mais aussi vingt-sept chefs d'État et de Gouvernement vont avoir à s'en accommoder.

Espérons que cette géométrie se pérennisera, car trouver un équilibre durable est une nécessité. Cela permettrait de dynamiser un organe - le Conseil européen - dont la perception dans l'opinion navigue entre une image d'institution affadie et la non-image. Dans le cas contraire, on risquerait de vérifier ce que Voltaire disait à peu près d'une assemblée déjà dévaluée à son époque: "Ils sont la-dedans 27, qui ont de l'esprit comme quatre." ☹

l'Académie française

²JO de l'UE du 20 aout 2009 - directive 2009/81/CE



De la mission rayonnement de la DMA à la section carrière du CGARm...

par **Daniel Reydellet**

A un moment où l'avenir de la section carrières du conseil général de l'armement semble incertain, il est intéressant de se pencher avec Daniel Reydellet, ancien secrétaire général du Conseil Général de l'Armement, sur plus de quarante années au service de la diversification du parcours professionnel des ingénieurs et officiers des corps de l'armement.

Un besoin ancien et reconnu : la mission rayonnement de la DPAG

Le besoin d'aide à la mobilité n'est pas spécifique des corps militaires de l'armement. Il existe dans tous les corps de l'Etat, civils ou militaires. La DMA en a pris conscience très tôt, puisque dès 1969 fut créée au sein de la DPAG "la mission rayonnement". A noter au passage que, dès le départ, la séparation géographique des deux entités a été considérée comme essentielle. Par ailleurs, le poids, l'expérience et la personnalité des Chargés de Mission Rayonnement successifs étaient un gage d'une certaine indépendance vis-à-vis de la DMA, puis de la DGA.

Trente ans après : intégration au Conseil Général de l'Armement : la Section Carrière

Il a toutefois fallu attendre 1999 pour que la Mission Rayonnement sorte de la DGA et soit rattachée, sous une nouvelle forme, la section carrière, au Conseil Général de l'Armement. Pendant 7 années, Louis Le Pivain a construit patiemment, mais avec le dynamisme qu'on lui connaît, un outil remarquable à l'écoute à la fois de chaque

individu des corps et des besoins des futurs employeurs... Enfin, Xavier Lebacqz a poursuivi l'ouvrage de 2006 à 2009.

Il n'est pas inutile de mesurer le chemin parcouru au sein du CGARm durant ces dix dernières années : constitution d'un référentiel documentaire unique sur toute question qu'un officier ou ingénieur des corps de l'armement peut se poser quant à sa mobilité, déploiement du réseau des employeurs éventuels afin de faire se rencontrer l'offre et la demande, publicité des différentes offres d'emploi, notamment sur le site Internet du CGARm, réalisations d'innombrables entretiens individuels, mise sur pied d'une base de données sur tous les personnels des corps de l'armement, comportant notamment l'historique des divers entretiens individuels...

Parallèlement, le Conseil Général de l'Armement évoluait également puisque lui étaient confiées par décret en 2006 "les orientations générales concernant les corps militaires de l'armement, notamment en matière de recrutement, d'emploi et de formation initiale et continue" : à côté de l'approche individuelle de la section carrière,

le CGARm donnait de l'ampleur à son approche collective et stratégique de la gestion des corps.

Et maintenant ?

Avec la nomination récente de Jean-Paul Herteman comme Vice-Président du Conseil Général de l'armement, une ère nouvelle s'ouvre. Il s'agit d'affronter des nouveaux défis, dans un monde où la mobilité professionnelle est plus que jamais la règle générale.

La "transformation" devient le slogan de base... mais n'oublions pas de capitaliser sur l'expérience... car, comme le dit une vieille chanson issue du vieux terroir du rugby :

"les grandes équipes ne meurent jamais"

L'esprit de la Mission Rayonnement, de la Section Carrière, à savoir "le catalyseur de mobilité" est de cette trempe... de cette matière indestructible apte à créer une nouvelle flamme à partir de ces cendres ...pour le plus grand bien individuel et collectif des corps de l'armement. ☺



DCI

L'esprit partenaire



Au cœur de votre stratégie défense et sécurité

Depuis plus de 37 ans, Défense Conseil International (DCI) opère dans le cadre fixé par le ministère de la Défense en étroite liaison avec les Etats-Majors et la DGA.

Spécialisée dans le transfert du savoir-faire militaire français, DCI garantit une compréhension globale des besoins de ses partenaires et leur apporte la solution la mieux adaptée en matière de formation, d'assistance, de conseil et de maîtrise d'ouvrage.

www.groupedci.com

Une AG sous haute sécurité...



par **Philippe Roger**

Président de la CAIA

Notre Assemblée Générale du 18 mai était remarquablement clairsemée, et on a même pu craindre, pendant que de trop rares et tardifs camarades descendaient (“l’ai-je bien descendu ?”) les marches de l’Amphi Renard, d’avoir plus de monde sur l’estrade, où se trouvaient entre autres deux générations de présidents et de trésoriers, que dans la salle.

Désespoir donc, après la séance, des nouveaux élus, Conseil, Bureau, et président, se constatant moins sexy que l’équipe précédente, et regrettant que si peu de camarades aient pu s’associer à l’éloge de Béatrice Charon, écouter son dernier -jusqu’à nouvel ordre !- exposé, apprécier l’assurance de notre benjamine et trésorière Julie Morvant, et participer au débat final avec nos invités.

Ceci jusqu’à ce qu’un coupable désigné apparaisse :

L’informatique, cette pelée, cette galeuse,

et même, thème de cette revue oblige, la sécurité informatique.

Il semble en effet que notre politique d’envoi de convocations par mail à tous ceux dont nous avons l’adresse ait abouti à un rendement très faible à la DGA, le message ayant du mal à traverser les passerelles du ministère.

Pour vérifier ce circuit, et informer ceux qui n’auraient pu lire les PJ., nous allons donc renvoyer à ceux dont nous avons le mail, que les intéressés nous en excusent, les projets de rapport moral et financier, ainsi qu’un CR de l’AG, par mail. Nous vous demandons de bien vouloir répondre, pour cette fois-ci en tous cas, afin d’accuser réception du message.

Le CR rapide de l’AG, que vous trouverez ci-après, sera complété dans la prochaine édition de la revue par un résumé du très intéressant débat sur l’évolution des corps

techniques et sur la concertation des associations de hauts fonctionnaires, mené par Jean Poulit, Président du G16, et Fabrice Dambrine, Président de la Fédération des grands Corps Techniques de l’Etat.

Retenons deux bonnes nouvelles annoncées en séance :

- la Fédération présidée par Fabrice Dambrine ayant modifié ses statuts, qui ne lui permettaient d’admettre que des associations représentant des corps civils, nous pouvons y présenter notre candidature, ce que j’ai fait dès le lendemain de l’AG.

- la DGA/DRH ayant recréé un bulletin trimestriel des mutations, promotions et décorations, cousin du cahier jaune de feu la revue “l’Armement”, nous autorise à l’aider à le diffuser à l’extérieur, ce que nous faisons dès la présente livraison. 📧

Deux présidents et deux trésoriers pour une AG



par **Julie Morvant**

Trésorière de la CAIA

*X promo 2005, formation ENSTA Architecture Navale.
En poste au CATOD en septembre prochain.*

L'assemblée générale s'est tenue le mardi 18 mai à l'ENSTA. Elle s'est ouverte sur une assemblée générale extraordinaire qui a approuvé la modification des statuts de l'association. Cette modification permet à un président élu lors de son deuxième mandat d'être rééligible à l'issue de ce dernier, pour quatre ans. Ceci permet au président d'assurer ses fonctions dans la durée, idéalement de 4 à 6 ans.

L'assemblée générale ordinaire a ensuite débuté sur l'approbation du procès-verbal de l'assemblée générale du 21 avril 2009 et sur l'ouverture du vote sur le renouvellement des membres du Conseil. Les candidats proposés par le Conseil et élus par l'assemblée générale sont les suivants :

- Didier Brugère - Jérôme De Dinechin
- Benjamin Gallezot - Julie Morvant
- Anne Diaz De Tuesta
- Patrick Defranoux - André Portalis
- Patrick Guyonneau - Philippe Hervé
- Arnaud Vandamme - Arnaud Salomon

Une fois n'est pas coutume, deux présidents se sont ensuite succédés pour présenter le rapport moral. Béatrice Charon, Présidente jusqu'en octobre, a rappelé l'importance de la solidarité et des liens de camaraderie qui nous unissent. Elle a également rappelé toutes les actions qui ont été menées en 2009 afin de participer au renom du corps de l'armement (colloque, gala, revue, etc.). Philippe Roger, actuel Président, a quant à lui mis l'accent sur deux grands axes de

travail qui orienteront l'année 2010 et les suivantes. Le premier concerne la défense des intérêts des membres du corps de l'armement, que ce soit pour des camarades en difficulté, pour le recrutement, ou l'avancement. Le second axe est davantage dirigé vers la fonction "armement" pour maintenir son efficacité et sa cohérence, en particulier en s'intéressant à l'avenir de notre corps et en organisant des réunions professionnelles (par exemple sous la forme de petits-déjeuners).

Là encore un peu d'originalité dans le déroulement de l'assemblée car ce sont deux trésoriers qui ont présenté le rapport financier. Laurent Mercier, ancien trésorier, a d'abord insisté sur le bilan très positif de cette année : les dépenses du colloque ont été inférieures à la prévision, le gala a été bénéficiaire et le portefeuille de l'association n'a pas été touché par la crise. Puis il a mis en évidence que le nombre de cotisants a fortement baissé en 2009. Julie Morvant, actuelle trésorière, a souligné que le gala se ferait avec un budget inférieur cette année, afin de tenir compte de la crise financière. Elle a également insisté sur la baisse du nombre de cotisations, seules ressources de l'association, baisse pouvant être due à l'abandon des courriers postaux.

A l'issue de ces présentations, les rapports moral et financier ont été approuvés par l'Assemblée Générale. Celle-ci s'est poursuivie par les interventions de Fabrice

Dambrine, Président de la Fédération des Grands Corps Techniques de l'Etat et Président du Syndicat des ingénieurs du Corps national des Mines, de Jean Poulit, Président du Groupe des Associations de la Haute Fonction Publique (G16), et de Philippe Roger, notre actuel Président. L'intervention, ponctuée de témoignages et d'anecdotes de la part des intervenants eux-mêmes comme de camarades de l'assemblée, a mis l'accent sur l'avenir des grands Corps techniques de l'Etat et sur les conclusions du rapport Folz-Canepa.

L'assemblée générale s'est terminée par un conseil qui a approuvé la composition du bureau et enfin, par un cocktail très convivial.



Votre nouveau bureau

- **Philippe Roger**, président
- **Yves Demay**, Vice-Président gala
- **Xavier Lebacqz**, Vice-Président associations
- **Jérôme De Dinechin**, Vice-Président communication
- **Sarma Gadjendra**, Secrétaire Général
- **Julie Morvant**, Trésorière
- **Didier Brugère**,
- **Olivier Robert**,
- **Emmanuelle Plessiet**,
- **Philippe Logak**

SCORPION :

Une évolution majeure de la conduite de projet dans le domaine terrestre



par **Jérôme LEMAIRE**

Ingénieur en chef de l'Armement
Chef de la Division Système de Combat de l'ETAS

Architecte de capacité Engagement Combat au SASF depuis mi 2007. Ingénieur ENSIETA, Docteur Sup'Aéro, il travaille d'abord dans le domaine de la robotique à l'ONERA Toulouse puis au GESMA. Il rejoint le SPART fin 2001 comme chef de projet "BOA", puis est nommé fin 2004 chef de la division Système de Combat de l'ETAS.

Le programme SCORPION vise à renouveler les moyens du combat de contact de l'armée de terre en fournissant un système de combat cohérent et intégré. Il doit répondre aux besoins d'adaptation des forces aux opérations actuelles et futures, et au renouvellement d'un parc blindé vieillissant. SCORPION constitue une étape majeure pour l'Armée de Terre en termes technico-opérationnels et capacitaires. Pour la DGA, l'enjeu réside dans l'évolution sur la manière de conduire la conception et la réalisation des systèmes complexes dans le domaine terrestre.

Genèse et introduction

La vision du "combat de contact futur" a été guidée depuis le début des années 2000 par le concept de la "Bulle Opérationnelle Aéroterrestre" (BOA) (Plan Prospectif à 30 ans, version 2001). Prenant en compte les évolutions du contexte opérationnel (symétrie / dissymétrie / asymétrie) et les évolutions permises par les technologies (systèmes d'information, robotique, protection active...), ce concept souligne également que la supériorité opérationnelle ne provient pas d'un système majeur mais de l'association judicieuse de différents systèmes. Suite à ces travaux conceptuels, le stade de préparation de l'étape 1 de SCORPION a

été l'occasion d'un important travail d'équipe entre l'EMA, l'EMAT et la DGA entre mi 2005 et fin 2009.

Périmètre de SCORPION et GTIA

Les unités du combat de contact, cœur de l'engagement au sol et des opérations actuelles, sont constituées en Groupements Tactiques Interarmes (GTIA), formés à partir des régiments d'infanterie, de cavalerie, du génie et d'artillerie. Leur capacité opérationnelle est déterminée par leurs moyens principaux de combat (combattants, plates-formes armées, équipements individuels et collectifs) et leur aptitude à les combiner (systèmes d'information et de combat).

SCORPION prend en compte à la fois la rénovation de systèmes existants et l'intégration progressive de nouveaux systèmes et équipements¹. Si les systèmes faisant partie du GTIA ont vocation à intégrer le périmètre de SCORPION peu à peu, il a été fait le choix de ne pas perturber des opérations déjà lancées alors même que les "normes" (labels) à respecter par les systèmes devant intégrer les unités SCORPION restent à préciser. La première étape de SCORPION a donc pris dans son périmètre les systèmes dont le renouvellement (VBMR et EBRC pour le VAB et l'AMX10RC), la modernisation (char Leclerc) ou la rationalisation (SICS pour les SIT et le SIR) étaient les plus urgents.

Mise en place de niveaux capacitaires

La mise en place de niveaux capacitaires correspond au besoin de quantifier le niveau de performance obtenu par l'introduction de nouveaux systèmes, par la mise à niveau de systèmes existants et par la combinaison de ces différents moyens. Il est prévu de mesurer ces niveaux capacitaires sur une instance représentative du système de systèmes d'au minimum un volume équivalent à un GTIA.

La mise en place des premiers niveaux capacitaires a demandé un travail d'architecture important entre l'EMA, l'EMAT et la DGA notamment en raison de son caractère novateur. Dans l'état actuel des prévisions, une démonstration de combat collaboratif (DCC) permettra de montrer le niveau de performances accessible à court terme en 2012. Puis, les jalons seront concrétisés par l'atteinte de trois niveaux capacitaires SCORPION (NCS) :

- NCS 0 - 2014 : rationalisation des systèmes d'information tactique avec SICS V0, s'appuyant sur le renouvellement des moyens du combat débarqué en cours (VBCI, Félin) ;
- NCS 1A - 2017 : premier niveau de combat collaboratif avec SICS V1 et le système de communication CONTACT ; augmentation de la survivabilité des unités au contact avec le déploiement du VBMR et la rénovation du char Leclerc ;
- NCS 1B - 2020 : élargissement du combat collaboratif à l'ensemble des moyens du contact avec SICS V1 s'appuyant sur un plus large déploiement de CONTACT et la livraison d'une capacité de combat multirôle complète et cohérente avec l'EBRC.

Forme programmatique

Les différentes formes d'organisation programmatique envisageables ont été examinées : programme d'ensemble, opération d'ensemble et programme. Question triviale pour de nombreux projets, elle est légitime pour SCORPION en raison de la nature de son périmètre et de son

caractère incrémental.

Afin de disposer d'une direction de projet forte pour maîtriser la complexité, compte tenu notamment du nombre croissant de systèmes et d'interfaces, et sans pour autant sacrifier la visibilité technique, financière et calendaire offerte aux différentes parties prenantes, la mise en place d'un programme disposant d'une réelle autorité à l'intérieur de son périmètre a été recommandée. La forme incrémentale doit permettre de disposer de résultats à des échéances raisonnables pour éviter l'effet "tunnel" de certains grands programmes.

Partage des travaux entre l'Etat et l'industrie

Le développement d'un système de systèmes comme SCORPION depuis l'allocation différenciée des capacités (observation, désignation, feux, protection) au sein du GTIA, jusqu'à la qualification technico-opérationnelle d'ensemble du système "GTIA SCORPION" nécessite la mise en place d'une structure étatique et industrielle forte.

La complexité de SCORPION rend difficilement envisageable de mener ce projet sans une contribution industrielle au niveau Système de Systèmes. La solution de type bureau d'études (retenue par les britanniques pour le projet FRES avec le bureau d'études Atkins) a été écartée, ce type de solution ne fournissant pas d'engagement significatif de l'industrie. A l'opposé, une solution de type Maître d'œuvre d'Ensemble apparaît comme peu réaliste en raison du poids des systèmes existants, mais également de l'importance des risques à supporter par l'industrie et par voie de conséquence du coût pour la maîtrise d'ouvrage. La remise en cause des contrats de type LSI (Lead System Integrator) aux Etats-Unis (cas du FCS) est de nature à confirmer ces craintes.

La solution de l'architecte intégrateur apparaît comme la réponse la plus équilibrée à la problématique de cohérence d'ensemble, de respect des rôles au niveau

système et système de systèmes, de maîtrise des coûts et de partage des risques entre la Maîtrise d'ouvrage et «l'industriel SCORPION». L'Etat reste maître de la réalisation des opérations constituantes majeures en étant le client direct des MOI systémiers en charge des opérations constituantes majeures. L'Etat conserve une partie des risques sur la réalisation globale de SCORPION et garde la maîtrise du déroulement des opérations constituantes.

Perspectives

Le Dossier de Lancement de la Conception (DLC) a été présenté le 22 février 2010 en comité ministériel d'investissement. Le stade d'élaboration est maintenant lancé. Les travaux vont permettre d'optimiser, sous les contraintes financières et calendaires fixées, les performances technico-opérationnelles des GTIA pour les premiers niveaux capacitaires et de finaliser les spécifications des différents systèmes mais également de sous-systèmes clé comme la vétronique. La maîtrise des interfaces entre les différents systèmes sera également un aspect important des travaux avec l'idée d'examiner les communautés qui sont possibles et pertinentes entre différents systèmes.

Pour accroître la pertinence des travaux d'architectures et participer à la maîtrise de la complexité, la maîtrise d'ouvrage pourra s'appuyer sur un architecte industriel. Cet architecte appliquera une méthodologie d'ingénierie système pour proposer des orientations et architectures, qu'il appartiendra à la Maîtrise d'ouvrage de juger pour en retenir les éléments à appliquer. Bien entendu, un tel programme ne saurait porter ses fruits sans des équipes étatiques (DGA + armée de terre) organisées et convenablement dimensionnées. ☺

¹ Longtemps, le projet américain FCS (Future Combat System) avait pris la voie d'un programme renouvelant entièrement des unités et livrant de nouvelles brigades "clé en main".



EDEN

*European Defense Economic Networks
Rhône-Alpes Initiative*

At Eurosatory 2010, discover, for the first time, the 42 SMES of EDEN (European Defense Economic Network) the First European Defense and Security Cluster.

Through EDEN, the 42 SMES members are able to develop a **secured network, to work together in order to provide integrated, innovative and competitive global solutions in 4 sectors:**

- Detection Protection and Surveillance
- Personal Protective Equipment
- Equipments for Aircraft, Ships and Ground Vehicles
- Qualification and Services

Visit EDEN on Stand n° F 521 Hall 6



**EDEN IS PARTNER OF THE EUROPEAN
DEFENSE SECURITY MEETINGS ,
ON MAY 2011,
AT LYON, FRANCE.**

More information on www.eden-defense-cluster.com

Quel genre de lecteur êtes-vous ?

Petit sondage pour nous aider à mieux manager notre magazine

Vous recevez régulièrement notre revue et avez constaté ses évolutions dans le temps. A l'origine simple bulletin de liaison, ce numéro 92 est aujourd'hui un magazine en couleur au dos cartonné, centré sur un dossier qui nous l'espérons, vous intéresse.

Mais justement, qu'en pensez-vous ? Voici une liste de questions qui ne devraient pas vous demander plus de cinq minutes pour y répondre, soit sous forme papier en nous renvoyant la présente feuille découpée ou scannée caia@caia.net, ou encore -ce qui sera plus simple à dépouiller- sur le site de la CAIA, www.caia.net.

Nous vous remercions d'avance de votre contribution, précieuse pour nous, et encore plus si vous acceptez de nous faire partager votre expérience pour écrire, pour participer à notre comité de rédaction ou accepter d'être interviewé.

En recevant le Magazine des IA

Quelle rubrique lisez-vous en premier

Vous lisez : presque rien la moitié presque tout

Dans les rubriques suivantes, vous lisez :

| | | | | |
|---------------------|-----------------------------------|----------------------------------|----------------------------------|---------------------------------|
| Europe | toujours <input type="checkbox"/> | souvent <input type="checkbox"/> | parfois <input type="checkbox"/> | jamais <input type="checkbox"/> |
| Lu pour vous | toujours <input type="checkbox"/> | souvent <input type="checkbox"/> | parfois <input type="checkbox"/> | jamais <input type="checkbox"/> |
| Camarades écrivains | toujours <input type="checkbox"/> | souvent <input type="checkbox"/> | parfois <input type="checkbox"/> | jamais <input type="checkbox"/> |
| Notes de lecture | toujours <input type="checkbox"/> | souvent <input type="checkbox"/> | parfois <input type="checkbox"/> | jamais <input type="checkbox"/> |
| Vie de la CAIA | toujours <input type="checkbox"/> | souvent <input type="checkbox"/> | parfois <input type="checkbox"/> | jamais <input type="checkbox"/> |
| Histoire des IA | toujours <input type="checkbox"/> | souvent <input type="checkbox"/> | parfois <input type="checkbox"/> | jamais <input type="checkbox"/> |
| Management | toujours <input type="checkbox"/> | souvent <input type="checkbox"/> | parfois <input type="checkbox"/> | jamais <input type="checkbox"/> |
| Carrière - profil | toujours <input type="checkbox"/> | souvent <input type="checkbox"/> | parfois <input type="checkbox"/> | jamais <input type="checkbox"/> |
| Technique | toujours <input type="checkbox"/> | souvent <input type="checkbox"/> | parfois <input type="checkbox"/> | jamais <input type="checkbox"/> |
| Lu au JO | toujours <input type="checkbox"/> | souvent <input type="checkbox"/> | parfois <input type="checkbox"/> | jamais <input type="checkbox"/> |
| Carnet pro | toujours <input type="checkbox"/> | souvent <input type="checkbox"/> | parfois <input type="checkbox"/> | jamais <input type="checkbox"/> |

Vous le conservez : moins d'une semaine un mois pour vos archives

A noter qu'il est possible de compléter sa collection en s'adressant à la CAIA pour des numéros plus anciens.

Management

Des rubriques que vous souhaiteriez trouver dans votre magazine

- | | | | |
|------------------------------------|--------------------------|--------------------------------------|--------------------------|
| L'ensemble des nominations DGA | <input type="checkbox"/> | Des expériences sympa en détachement | <input type="checkbox"/> |
| Le point sur des grands programmes | <input type="checkbox"/> | L'histoire des IA | <input type="checkbox"/> |
| Opportunités de carrière | <input type="checkbox"/> | Des livres propos vraiment libres | <input type="checkbox"/> |
| Des jeux ou récréations | <input type="checkbox"/> | Les ingénieurs de défense en Europe | <input type="checkbox"/> |

Autre.....

Vous préféreriez des articles : techniques uniquement technique et management

Les dossiers constituent le cœur de notre revue

- | | | | | | | | |
|--------------------------------------|--------------------------|------------------------|--------------------------|--------------|--------------------------|---------------|--------------------------|
| Vous les trouvez trop longs | <input type="checkbox"/> | Adaptés à vos attentes | <input type="checkbox"/> | Trop courts | <input type="checkbox"/> | | |
| Les sujets sont trop techniques | <input type="checkbox"/> | corrects | <input type="checkbox"/> | sans intérêt | <input type="checkbox"/> | | |
| Vous préféreriez davantage de sujets | | techniques | <input type="checkbox"/> | sociétaux | <input type="checkbox"/> | géopolitiques | <input type="checkbox"/> |

Suggestions de thèmes

Sur la forme, vous trouvez votre magazine

- | | | | | | | | |
|--------------------------------------|---|-------------------------------------|--------------------------|-------------------------|--------------------------|-------------|--------------------------|
| Trop long | <input type="checkbox"/> | bien et agréable | <input type="checkbox"/> | trop court | <input type="checkbox"/> | | |
| Le format actuel vous semble | | trop petit, il vaudrait mieux du A4 | <input type="checkbox"/> | bien, à conserver | <input type="checkbox"/> | | |
| La typo est | difficile à lire <input type="checkbox"/> | correcte | <input type="checkbox"/> | agréable | <input type="checkbox"/> | | |
| Vous trouvez en général les articles | | trop longs | <input type="checkbox"/> | bien dimensionnés | <input type="checkbox"/> | trop courts | <input type="checkbox"/> |
| La mise en page vous semble | | banale | <input type="checkbox"/> | belle, aérée et moderne | <input type="checkbox"/> | ringarde | <input type="checkbox"/> |

Les auteurs

- | | | | | | | | |
|----------------------------------|--------------------------|-----------------|--------------------------|----------------------|--------------------------|--------------|--------------------------|
| Bien choisis | <input type="checkbox"/> | trop d'IA | <input type="checkbox"/> | propos trop convenus | <input type="checkbox"/> | | |
| Les biographies sont, pour vous, | | trop détaillées | <input type="checkbox"/> | bien | <input type="checkbox"/> | trop courtes | <input type="checkbox"/> |

Acceptez-vous d'être interviewé par un rédacteur de la CAIA, et sur quel thème :

- | | | | | | |
|--|--|-----|--------------------------|-----|--------------------------|
| Vous souhaiteriez retrouver tous nos articles sur le site internet : | | oui | <input type="checkbox"/> | non | <input type="checkbox"/> |
| Vous êtes déjà allé sur notre site internet | | oui | <input type="checkbox"/> | non | <input type="checkbox"/> |
- (si non, c'est le moment de le faire pour mettre vos coordonnées à jour, non ?)

Dernière question, quelles seraient vos suggestions pour notre magazine :

.....
.....

Enfin, si vous souhaitez nous faire partager votre expérience pour rédiger, interviewer, choisir, n'hésitez pas à nous faire signe caia@caia.net (Nous nous réunissons une fois par mois, entre 12h15 et 14 h à l'ENSTA).

C'est déjà fini, un grand merci pour votre collaboration.

Le comité de rédaction



www.sominex-defense.fr

■ Etude et fabrication...

■ Expertise en test balistique...

■ Projets spéciaux...



Sominex, c'est aussi :

Sominex Sciences : équipements high-tech pour les laboratoires de recherches en physique

Sominex Energies : équipements pour la prospection pétrolière, le nucléaire et le renouvelable

Sominex Industries : électronique haut de gamme à forte contrainte, hydraulique et maintenance



« La société Sominex, créée en 1976, intervient dans les secteurs de hautes technologies avec une offre de services entièrement intégrée. Expertise approfondie, qualité, service... sont nos préoccupations quotidiennes pour répondre à vos besoins ».

Jean-Jacques BENOIT
Président



Siège Social :

Zone Industrielle - 13 rue de la Résistance - BP 61620 - F-14406 BAYEUX cedex
Tél. : +33(0)2 31 61 40 00 - Fax : +33(0)2 31 92 98 22
www.sominex.fr

Enigma et les progrès de la cryptanalyse

par **Daniel Jouan**

Ingénieur général de l'Armement

La cryptographie est connue depuis la plus haute Antiquité, mais son utilisation au cours de la Seconde Guerre mondiale lui a fait atteindre le rang d'une science à part entière. Corrélativement, l'analyse des codes secrets et des moyens de les "casser", c'est-à-dire la cryptanalyse, a connu au cours de cette période des progrès fulgurants. Ils ont certainement influencé de façon déterminante le cours de la guerre et permis d'accélérer les connaissances dans les sciences de l'information.

La cryptographie ne date pas d'hier ! Le premier document chiffré connu remonte à l'Antiquité. Une tablette d'argile retrouvée en Irak, datée du XVI^e siècle avant J.C., porte la recette d'un potier. Ce dernier y avait supprimé des consonnes et modifié l'orthographe des mots afin de garder secret son processus de fabrication.

Depuis, les méthodes ont connu bien des progrès. Par exemple, les hébreux chiffrèrent les textes religieux par la méthode de substitution alphabétique inversée (chaque lettre du texte en clair est remplacée par celle qui a le même rang dans l'alphabet en ordre inverse : A est remplacé par Z, B par Y, etc.). Les premiers véritables systèmes de cryptographie datent du deuxième siècle avant J.C. Ce sont essentiellement des chiffrements par substitution : mono-alphabétique (chaque lettre est remplacée par une autre lettre de l'alphabet), poly-alphabétique (la règle de substitution varie d'une lettre à la suivante

selon une clé réutilisée périodiquement), polygrammatique (un groupe de caractères est remplacé par un autre groupe de caractères).

Avant la Seconde Guerre mondiale

La cryptographie ne concerne pas seulement la politique et la guerre. Pour protéger les projets industriels et les relations commerciales, de nombreuses études ont été conduites dès le début du XX^e siècle afin d'assurer la confidentialité des messages. En 1919, un ingénieur hollandais, Hugo Alexander, dépose un brevet de machine à chiffrer électromécanique. Les idées sont reprises à Berlin par le Docteur Arthur Scherbius qui monte une société destinée à fabriquer et à commercialiser une machine à chiffrer à usage civil appelée Enigma. Cette société est un échec, mais la machine Enigma a attiré l'attention des militaires. Ces derniers vont analyser le fonctionnement de cette

machine et l'améliorer à des fins stratégiques.

Le principe de fonctionnement d'Enigma

Enigma est une machine électromécanique utilisant des composants mécaniques et électriques. Son principe repose sur le passage d'un courant électrique à travers une série de câblages portés par des rotors. Les premières machines étaient composées de trois rotors, mais les militaires allemands en ajoutèrent deux autres par la suite. Les câblages des rotors sont spécifiques et différents. Après le passage dans les trois rotors, le courant arrive dans un réflecteur qui le renvoie dans les rotors en sens inverse, et la substitution de la lettre se concrétise par l'allumage d'une lampe. Une même lettre ne peut jamais être codée par elle-même. Afin de complexifier le fonctionnement, chaque rotor peut tourner. L'appui sur une touche du clavier fait tourner le premier

rotor d'un incrément. Le second tourne à son tour après la rotation complète du premier rotor et ainsi de suite.

Les essais de décryptement d'Enigma avant la guerre

Dès 1920, les services polonais commencent à travailler sur le décryptement des transmissions chiffrées allemandes, interceptées par leurs services de renseignement. En 1929, une erreur lors de l'envoi de Berlin à Varsovie d'une machine Enigma par la valise diplomatique permet aux Polonais de se procurer un exemplaire de la machine. Les services secrets vont en examiner le mode de fonctionnement. La version interceptée est une version commerciale simple, mais l'examen confirme que les allemands utilisent une telle machine pour coder leurs messages militaires. Lorsque toute l'armée allemande utilisera cette machine quelques années plus tard, les Polonais se douteront qu'il s'agit d'une variante améliorée d'Enigma.

Commence alors une cryptanalyse approfondie visant à trouver le mode de câblage utilisé dans la version militaire et d'en déduire les clés permettant de déchiffrer les messages interceptés.

Marian Rejewski, mathématicien polonais de 27 ans, découvre un moyen mathématique pour retrouver le câblage de la machine et la clé permettant de déchiffrer les messages. Il remarque que, dans les messages interceptés, les opérateurs militaires utilisent des chiffres redondants ; ceux-ci choisissent un mot très court (en général trois lettres) et le répètent une fois au début du message, ce qui leur permet de caractériser les procédures en vigueur

lors du chiffrage. Par une étude attentive des débuts de message, M. Rejewski constate que les codages différents d'une même lettre sont liés de façon étroite par la rotation des rotors. Même si les trois lettres originales sont inconnues, le nombre de câblages qui peuvent les transformer en une séquence particulière sont limités. Rejewski les nomme des "chaînes".

La cryptanalyse va alors consister à trouver les bonnes chaînes. L'interception d'un vieux manuel d'Enigma va permettre un nouveau progrès.

En étudiant attentivement ce manuel, Rejewski arrive à la conclusion que le nombre de chaînes possibles atteint 105 456, ce qui, avec les moyens de calcul de l'époque, ne permet pas de trouver les clés recherchées en un temps raisonnable. Les méthodes alors utilisées sont graphiques et sont basées sur des grilles transparentes que l'on superpose et qui permettent d'éliminer les chaînes impossibles. Les Britanniques utilisaient des méthodes semblables, bien adaptées pour la machine Enigma commerciale, mais pas pour la machine améliorée par les militaires allemands.

Pour améliorer le temps de recherche, les polonais vont mettre au point en 1938 une "bombe cryptologique", véritable ordinateur électromécanique. Six exemplaires de cette bombe seront montés à Varsovie juste avant le début de la Seconde Guerre mondiale. Le volume de ces installations est considérable et équivalent à un atelier de 100 personnes, mais les performances sont à la hauteur puisqu'on arrive à obtenir une clé au bout de deux heures.

Une bonne partie des transmissions de

l'armée allemande pourront alors être décryptées dès 1933 et jusqu'à l'aube de la Seconde Guerre mondiale.

Les aléas des recherches pendant la Seconde Guerre mondiale

En 1939, les Polonais se rendent compte que les progrès des Allemands en matière de cryptographie sont devenus trop importants. Avec la guerre qui va débiter, les Allemands ont introduit deux rotors supplémentaires. Peut-être parce que le contre-espionnage allemand était informé des méthodes employées par la Pologne pour casser les codes, le principe de répétition du code en début de message est abandonné ce qui réduit à néant les efforts réalisés.

Les Polonais partagent alors le fruit de leurs travaux avec les Français et les Britanniques. Ils fournissent durant l'été 1939 des copies d'Enigma, la description des méthodes d'analyse et les plans de la bombe cryptographique. En septembre 1939, l'invasion de la Pologne par les nazis à l'ouest et les soviétiques à l'est oblige les cryptologues polonais à évacuer leurs bureaux dans l'urgence. Ils atteignent Paris et se mettent au service de la France. De passage à Paris, le mathématicien anglais Alan Turing prendra connaissance des travaux déjà réalisés.

Au Royaume-Uni, les opérations de décryptement sont conduites dans un contexte purement britannique et américain. La méthode polonaise ne fonctionnait plus sur les versions militaires d'Enigma, et ne fonctionnait pas sur la version Marine de la machine qui avait toujours été supérieure en termes de sécurité. Les Polonais ne s'étaient pas vraiment intéressés à

Histoire

l'interception des transmissions navales, alors que celles-ci présentaient une importance capitale pour les marines alliées.

C'est Alan Turing qui va s'occuper de l'analyse de la machine Enigma en version navale. Ses bureaux sont installés à Bletchley Park, manoir proche de Londres où sont retranchés tous les cryptanalystes et mathématiciens alliés. Avec Gordon Welchman, ils seront à l'origine du déchiffrement total d'Enigma.

L'attaque des Britanniques est basée plus particulièrement sur le réflecteur, élément qui garantit que toute lettre est nécessairement différente après chiffrement. De plus, ils font appel à une technique d'analyse basée sur les mots "probables". Ainsi, le raisonnement tenu consiste à supposer que des termes comme "Heil Hitler", "Führer", "Stuka", etc, ont de fortes chances de figurer dans les messages interceptés. Ces estimations du contenu des messages étaient appelées des cribles. Une corrélation avec les opérations militaires du moment permettait aussi de faciliter l'élaboration de ces cribles. Avec quelques hypothèses sur le contenu, il devenait possible de retrouver une partie du message en essayant quelques chaînes vraisemblables. A partir des résultats positifs, on arrivait à retrouver le texte complet.

Les opérateurs allemands aidèrent involontairement les cryptanalystes. Il arrivait qu'on leur demande d'effectuer un test en envoyant un message ne comportant que des T, ce qui entraînait à la réception un

message sans T qu'il était facile de reconnaître. Certains opérateurs utilisaient aussi souvent les mêmes paramètres en début de message, par exemple les initiales d'un proche, système facilement identifiable après quelques messages. D'autres ajoutaient un en-tête constant selon le type de message, par exemple WET (de wetter, temps météo) s'il s'agissait de rapport météo, sujet sur lequel les exigences de secret paraissaient moins importantes, ce qui permettait d'avancer dans la connaissance des clés de la machine utilisée.

Si les Allemands avaient changé les rotors plus souvent, il est possible que les efforts des experts de Bletchley Park soient restés vains. Mais l'envoi de nouveaux rotors demandait une logistique difficile à déployer à ce stade du déroulement de la guerre. Il fallait en effet s'assurer que tous les navires étaient simultanément en possession des mêmes rotors. C'est pourquoi les allemands préférèrent ajouter des rotors sans modifier les autres en particulier pour le chiffrement des transmissions de marine.

Face au danger et au risque d'une défaite dans la bataille de l'Atlantique, les alliés mirent sur pied plusieurs opérations pour dérober les carnets de code allemands. Certaines virent le jour, d'autres restèrent à l'état de projet. La chance leur sourit en 1942. Le H.M.S. Gleaner intercepta l'U-33 alors qu'il allait poser des mines dans un chantier portuaire britannique. Le Gleaner largua des mines sous-marines sur le sous-marin allemand ce qui le força à faire surface. Bien que le commandant du sous-marin ait commandé le sabordage du navire, on n'eût

pas le temps de jeter les rotors de la machine Enigma à l'eau. Les Britanniques purent ainsi mettre la main sur ces pièces, ce qui permit des progrès rapides dans le décryptement des messages chiffrés allemands.

Les conséquences des recherches effectuées

Ce succès en matière de renseignements militaires influença fortement le cours de la Seconde Guerre mondiale. La capacité des alliés à décrypter les transmissions de la marine italienne (qui utilisait aussi Enigma) leur donna l'avantage lors de la bataille de Matapan (au large de la Crète) et écarta la menace italienne de la Méditerranée. Les informations décryptées permirent aussi de connaître à l'avance les mouvements des troupes de Rommel en Afrique du Nord, l'empêchant ainsi de rentrer en Egypte et de contrôler la côte méditerranéenne d'Afrique du Nord.

C'est par le décryptement des messages que l'on apprit que les fusées V1 étaient construites à Peenemünde en Allemagne, entraînant plusieurs opérations militaires destinées à détruire les usines. Il est également certain que les opérations de débarquement de juin 1944 en furent d'autant facilitées.

Enfin, les travaux d'Alan Turing dépassèrent largement le domaine de la cryptanalyse puisqu'on peut considérer qu'ils accélèrent les recherches de mise au point des calculateurs électroniques.





Module de Surveillance Environnementale (MSE):

La solution globale de 3^e génération de détection et d'alerte pour la gestion du risque Nucleaire Radiologique Bacteriologique Chimique.



- Ensemble intégré, labélisé par le Pôle de Compétitivité Gestion des Risques et Vulnérabilités des Territoires de la région PACA.
- Détection isotopique innovante α , β , γ , X et neutrons.
- Détection biologique par fluorescence et collecte d'échantillons sous forme d'aérosol ($1 \text{ à } 10 \mu\text{m}$).
- Détection chimique des toxiques de guerre et des toxiques industriels.
- Transmission de la position GPS, de la modélisation numérique et des données météo en temps réel vers le Poste de Commandement.
- Utilisation dans des conditions climatiques extrêmes (-32°C à $+55^\circ\text{C}$).



Pour plus d'informations: www.biolabh2o.com

Rendez-nous visite du 14 au 18 juin 2010 :

EUROSATORY
 HALL 5 STAND U431

BIOLAB H2O
 400 avenue Roumanie
 B.P.309-84x 7
 Sophia Antipolis
 05805 BiOT Cedex-France
 Tél.: 33(0)4 42 66 05 92
 Fax: 33(0)4 42 66 02 92

SURVEY
weControl

You dream of a customized equipment.
SURVEY Copter will design and realize it for you tomorrow.
www.survey-copter.com

Des métiers d'avenir à l'international :
une formation spécialisée de l'ICP («la Catho»)

LE MASTER DE RELATIONS EUROPÉENNES ET LOBBYING

LE DIPLÔME D'ÉTUDES SUPÉRIEUR EST :

- EN **1 AN** (ACCÈS DIRECT APRÈS **BAC+4**, OUVERT À TOUTES SPÉCIALITÉS)
- EN **2 ANS** (APRÈS **BAC+3**, TOUTES SPÉCIALITÉS) EN PASSANT PAR LE M1 DE GÉOPOLITIQUE ET RELATIONS INTERNATIONALES

SES AVANTAGES :

- DES ENSEIGNEMENTS ORIENTÉS VERS LA PRATIQUE ET LES DÉBOUCHÉS
- DES PARTENARIATS AVEC DES ACTEURS DU MONDE ÉCONOMIQUE
- UN STAGE LONG EN MILIEU PROFESSIONNEL
- CE **DIPLÔME** DONNE AUX « JUNIORS » LES **ATOUTS** POUR ACCÉDER À UN **MONDE DU TRAVAIL** ACTUELLEMENT DIFFICILE

Informations et dossier sur www.icp.fr - Candidatures jusqu'au 15 juillet - Directeur : Michel Clamen

Mission d'un cryptologue français en Russie (1916)

d'Henry Olivari - Editions de l'Harmattan, 2009



Le lieutenant-Colonel Olivari, polytechnicien, champion d'échecs et officier du 2^{ème} bureau, est envoyé en Russie en 1916 en mission spéciale pour apprendre aux russes à écouter puis déchiffrer les messages sur le front allemand. Dans cette chronique d'une période charnière pour l'Europe, Henry Olivari décrit les ambiances, les personnes, les lieux avec une précision et une acidité toute particulière. On y rencontre l'ambassadeur et futur académicien français Maurice Paléologue qui relate par ailleurs cette époque dans "la Russie des tsars pendant la grande guerre", l'ambassadeur l'anglais Lord Buchanan, des politiques et militaires russes et de l'Europe entière. La mission n'est pourtant pas aisée, autant par les tracasseries administratives françaises que russes, par la lenteur des communications, par les intérêts contradictoires des personnes. Il faut un concours de circonstances particulier pour que l'autorisation d'aller

sur le front soit donnée. Sur place, les postes d'écoute n'entendent initialement que les communications russes, les lignes allemandes étant doublées et blindées... Cependant, la mission s'interrompt au bout de quelques mois, et Olivari revient à Paris chargé de transmettre une inquiétude sur le plan politique, porteur d'un code secret allemand OABU chemisé dans du plomb pour pouvoir être jeté à la mer en cas d'arraisonnement. Le message politique qui contredit les messages officiels ne sera pas entendu. Olivari apprend que le code est déjà possédé par le chiffre français, que sa mission a été torpillée depuis Paris et qu'il ne retournera pas en Russie. C'est avec amertume qu'il demandera sa mutation... Cahiers de souvenirs personnels non destinés à être publiés, ces mémoires donnent un éclairage subjectif passionnant à la veille de la révolution russe. 📖

JDD



Histoire des codes secrets

de Simon Singh

Le livre de poche, 2001

Bien que ne datant pas d'hier, le livre de Simon Singh, journaliste et physicien se lit comme un roman. Il explique les codes secrets utilisés dans le domaine de la guerre et de l'espionnage depuis l'antiquité jusqu'aux algorithmes modernes RSA ou PGP en passant par la reine Mary Stuart et l'entrée en guerre des USA pendant la Seconde Guerre mondiale. Un livre qui donne l'impression de comprendre un domaine mathématique complexe, et de plus en plus utile aujourd'hui. 📖

JDD

Promotions et décorations

Information sur les mouvements dans l'Armement

La première lettre trimestrielle des officiers des corps de l'Armement est parue en mai 2010. En accord avec la DGA, nous en publions quelques extraits qui nous concernent particulièrement. Un bon moyen de rester en contact...

Promotions

• Ingénieurs de l'armement

Au grade d'ingénieur en chef (au 01/01/10) :

Sirapian Massis
Vieste Laurent
Germond Emmanuel
Lavarde Axel
Charlet Renaud
Marrel Thibaut
Filliat David
Sigaud Philippe
Lecarpentier Maud
Carcenac Claude
Lenglin Geoffroy

Au grade d'ingénieur principal (au 26/11/09) :

Lecoïnte Olivier
Goy Alexandre
Bouzeloc Corinne

Au grade d'ingénieur principal (au 01/01/10) :

Freyheit Charles
Gommard Guillaume
Vieu Emilie
Duveau Guillaume
De Seze Antoine
Theret Damien
Portier Maximilien
Dubois Vivien
Peudon Benoît
Lopez Laurent
Deloncle Axel
Mabile Laëtitia

Pleçis Adrien
Osmont Antoine
Lavergne Jérôme
Defossez Amans
Constancias Laurent
Borrod Jean-Sébastien

Au grade d'ingénieur (au 01/09/09) :

Longuet Baptiste
Germain Laurent
Kaller François

Décorations

• Légion d'honneur

Décret du 6 juillet 2009 portant promotion et nomination (JO du 7 juillet 2009)

Au grade de commandeur :

Collet-Billon Laurent (IGE)
Panié Jean-Paul (IGE)

Au grade d'officier :

Castellani Philippe (IG2A)
Châtenet Bruno (IG1A)
Chimot Jean-Marc (IG1A)
Codde Roland (IG1A)
Demay Yves (IG1A)
Dunaud Alain (IG1A)
Frachon Bruno (IG1A)
Houttemane Jean-Paul (IG1A)
Lusseyran Pierre (IG1A)
Royal Bernard (IG1A)

Au grade de chevalier :

Abguillerm Pierre (ICA)
Bernard Thierry (ICA)
Bruni Eric (ICA)
Buey Yves (IG2A)
Cariou Henri (IC1ETA)
Cau Jean (IC1ETA)
Charpentier Etienne (ICA)
Chevalier Yves (ICA)
Colin Yves (ICA)
Delapierre Jean (IC1ETA)
Durand Jean-Marie (IG2A)
Esnult Alain (ICA)
Fabrice Laurent (ICA)
Gallard Christophe (ICA)
Gérard Jean-Michel (ICA)
Inizan Christian (IC1ETA)
Laugier Patrick (ICA)
Le Boulch Pierre-Yves (IC1ETA)
Le Danff Jean (IC1ETA)
Le Stum Joël (ICA)
Leblond Thierry (ICA)
Leray Etienne (IC1ETA)
Mangiapane Jean-Luc (IC1ETA)
Ménard Gilles (IC1ETA)
Mondon Alain (IC1ETA)
Montet Thierry (IC1ETA)
Phalipaud Lionel (IC1ETA)
Pistoresi Marc (IC1ETA)
Portes Marc (IC1ETA)
Pujo Jean-Louis (IC1ETA)
Rasset Reynald (ICA)
Salmon Pierre (IG2A)
Sechet Caroline, épouse Laurent (IG2A)
Suc Sylvie, épouse Jacquemot (ICA)

Tavernier Caroline, épouse Gervais (ICA)
Tropato Jacques (OC1TAA)

• **Ordre national du mérite :**

Décret du 6 novembre 2009 portant promotion et nomination (JO du 8 novembre 2009)

Au grade de commandeur :

Auroy Patrick (IGH)
Delor Bruno (IGH)
Donzel Maxime (IGH)
Pène Jean (IGE)

Au grade d'officier :

Benâtre Frédéric, Maurice, René (IG2A)
Cousquer Jacques (IG2A)
Dill Michel (IC1ETA)
Fayol Pierre (IG2A)
Hélou Christian (IC1ETA)
Lefort Claude (IC1ETA)
Legrand Monique épouse Larroche (IG2A)
Miallet Séverin (IG2A)
Niec Patrick (IG2A)
Salvetti Vincenzo (IC1ETA)
Vinau Richard (IG2A)
Waringhem Eric (IG2A)

Au grade de chevalier :

Barale Thierry (IC2ETA)
Beffy Sylvie (OPCTAA)
Berni Jean-Erwan (ICA)
Bouchacourt Isabelle, épouse Tanchou (ICA)
Boulvert François-Régis (IC2ETA)
Carré Dominique (IC2ETA)
Chol Emmanuel (ICA)
Clamens Didier (IC2ETA)
Clouet Jean-François (ICA)
Conan Erwan (ICA)
Coum Hervé (IC2ETA)
Delpont Yvon (OC2TAA)

Demogeot Frédéric (IC2ETA)
Desit Franck (ICA)
Dupont Sophie, épouse Vacher (IC2ETA)
Fasquel Christophe (IC2ETA)
Francou Thierry (ICA)
Gibello Ghislaine (IC2ETA)
Grenard Patrick (IC2ETA)
Jeanne Jean-François (IC2ETA)
Jodet Lionel (ICA)
Kermarrec Jean-Yves (IC2ETA)
Kremer Eric (OC2)
Lars Bertrand (IC2ETA)
Le Goff Hervé (IC2ETA)
Le Goff Yann (IC2ETA)
Ledieu Laurent (IC2ETA)
Lemaire Jérôme (ICA)
Longépé Bernard (IC2ETA)
Mathieu Laurent (IC2ETA)
Ménissier Pierre (IC2ETA)
Mercier Laurent (ICA)
Mérijeau Hugues (IC2ETA)
Mirlier Anne (OC2TAA)
Parvillers Olivier (IC2ETA)
Pedron Christophe (IC2ETA)
Pichon Stéphane (ICA)
Raby Damien (ICA)
Rigal Jean-François (IC2ETA)
Rio Jean-Pierre (IC2ETA)
Rivoal Jean-Paul (IC2ETA)
Ruvira Pierre-Yves (IC2ETA)
Sévy Christine, épouse Houlot (OC2TAA)
Thomassier Vincent (ICA)
Toulliou Stéphane (IC2ETA)
Truffert Vincent (IC2ETA)
Vallet Stéphane (IC2ETA)
Ventos Philippe (IC2ETA)
Vu Quang (IC2ETA)

• **Ordre national du mérite**

Décret du 4 mai 2010 portant promotion et

nomination (JO du 6 mai 2010)

Au grade de commandeur :
Denais Paul (IGH)
Renvoisé Patrick (IGH)

Au grade d'officier :

Berville Marc (IG2A)
Combrisson Jean-Luc (IG2A)
Fagnen Roland (IC1ETA)
Legrand Marie-France,
épouse T'kint de Roodenbeke (IG2A)
Lelaizant Nathalie épouse Guillou (IG2A)
Maillet Fernand (IC1ETA)
Monvoisin Dominique (IG1A)
Wolf Philippe (IG2A)

Au grade de chevalier :

Cocheugue Catherine épouse Pradier (IC2ETA)
David Ronan (IC2ETA)
Drévilhon Jean-François (IC2ETA)
Dussol Jean-Pierre (IC2ETA)
Goeb Laurent (ICA)
Guilpin Xavier (IC2ETA)
Hamono Jean-Claude (IC2ETA)
Lefebvre Fabrice (ICA)
Mahler Olivier (IC2ETA)
Mérat Jean-Michel (IC2ETA)
Petit Frédéric (ICA)
Peyrichon Marc (ICA)
Pondaven Patrice (IC2ETA)
Trotin Eric (ICA)

• **Médaille de l'aéronautique**

Décret du 20 janvier 2010 portant attribution de la médaille de l'aéronautique au titre de de 2009 (JO du 9 janvier et du 17 février 2010)

Alphonsout Bruno (IPETA)
Kiert Willy (IPETA)

Promotions et décorations

Thomas Daniel (IPETA)
Valorge Christophe (ICA)

• Mérite maritime

Décret du 4 septembre 2009 portant nomination dans l'ordre du Mérite maritime

Au grade de chevalier :
Saliou Olivier (IC2ETA)

Mobilités et départs

• Mouvements de mars :

AGUESSE Thomas (ICETA)
DGA Techniques Terrestres - 1 mars 2010

BAILEY Hugh (IETA)
MINEIE - 1 mars 2010

BROSSE Guillaume (IETA)
DGA Ing projets - 1 mars 2010

CHILESE Christophe (IETA)
OTAN - 1 mars 2010

DAVID Ronan (ICETA)
PPE - 1 mars 2010

DOMMERGUE Aurélien (IETA)
DGA Maîtrise information - 1 mars 2010

DUFEY Christophe (IETA)
PPE - 1 mars 2010

FERMIER Patrick (IGA)
PPE - 1 mars 2010

GUILPIN Xavier (ICETA)
DP - 1 mars 2010

MAUREL Blaise (IETA)
UM ESIO - 1 mars 2010

OLIVIER Frédéric (IETA)

DGA Ingénierie projets - 1 mars 2010

PARIS Christophe (IETA)
DGA Ingénierie projets - 1 mars 2010

PERON Jean-Paul (ICETA)
DI - 1 mars 2010

PISTORESI Marc (ICETA)
INSP - 1 mars 2010

REICHART Arnaud (ICA)
ENSTA - 1 mars 2010

VOLPOET Ivan (IPETA)
DGA Essais en vol - 1 mars 2010

BERNARD Hervé (ICA)
MIP - 8 mars 2010

CAPLAIN Philippe (IGA)
INSP - 8 mars 2010

CORNET Henri (IGA)
DP - 8 mars 2010

LEGRAND ép T'KINT
DE ROODENBEKE Marie-France (IGA)
SMQ - 8 mars 2010

MORIGAUULT Arnaud (IA)
DRH - 8 mars 2010

ROTH Sylvain (ICA)
DGA - 11 mars 2010

CROZES Cyril (ICA)
DS - 15 mars 2010

MALEJAC Patrice (ICETA)
OCCAR - 15 mars 2010

MANGEOT Olivier (IPA)
DP - 15 mars 2010

MOYRET Pierre (ICA)

DS - 15 mars 2010

PONTAILLER Pascal (ICETA)
CAEPE - 22 mars 2010

SEZNEC Francis (ICETA)
DO - 31 mars 2010

• Mouvements d'avril :

BURLION Laurent (IETA)
ONERA - 1 avril 2010

CHEVILLOT Jean-Eric (IGA)
DGA Essais en vol - 1 avril 2010

CHOQUE ép BERNE Denise (OCCTAA)
DP - 1 avril 2010

COSTES Alain (IGA)
CGARM - 1 avril 2010

CROUZAT ép LOPEZ Aude (IA)
DP - 1 avril 2010

CRUCK Eva (IETA)
DS - 1 avril 2010

GAMBIER Franck (IPETA)
UM NAV - 1 avril 2010

GOUZOU Sébastien (IETA)
Ing projets - 1 avril 2010

LE BERRE ép CHAPELLE Stéphanie
(OPCTAA)
SEREBC - 1 avril 2010

LOPEZ Laurent (IA)
DGA Ing projets - 1 avril 2010

LUNEL Yves-Laurent (IPETA)
DGA Techniques Aéro - 1 avril 2010

MARY Olivier (ICETA)
UM RAF - 1 avril 2010

MILLION-PICAILLON Eric (ICA)
SMQ - 1 avril 2010

MONJAUZE Frédéric (IPETA)
UM MID - 1 avril 2010

PICHON Daniel (ICETA)
EMM - 1 avril 2010

PIRET Aurélien (IETA)
DGA Ing projets - 1 avril 2010

PUJOL Yves (IPETA)
SMCO - 1 avril 2010

REBERT Jean-Marc (ICA)
SIAé - 1 avril 2010

REICHARDT Michel (OCTAA)
DS - 1 avril 2010

ROTH Pierre-André (IGA)
DGA - 1 avril 2010

ROUX Gautier (IA)
EMM - 1 avril 2010

ZECCHINI Robert (ICETA)
INSP - 1 avril 2010

• **Retraite et 2^{ème} section :**

LARS Bertrand (ICETA)
1 mars 2010

POTIER Serge (ICETA)
1 mars 2010

TREHARD Luc (IGA)
31 mars 2010

DONZEL Maxime (IGA)
8 mars 2010

Formation

• **IHEDN :**

Auditeurs sélectionnés pour la Session nationale Armement et économie de défense 2010 :

Bezombes Patrick (ICA)
Carlier Mireille (ICA)
Catty Laurent (ICT)
Dagail Philippe (IC2ETA)
Dupuy Pierre-Yves (IC2ETA)
Le Yaouanc Yannick (ICA)
Longépé Bernard (IC2ETA)
De Maricourt Antoine (ICA)
Masson Jean-Philippe (ICT)
Pichon Stéphane (ICA)

Roger Denis (ICA)
Sayegh Michel (ICA)
Sellier Cécile (ICA)
Zecchini Robert (IC1ETA)

• **CID**

Auditeurs sélectionnés :

Vieste Laurent (ICA)
Ramaen Christophe (IC2ETA)
Colas Samuel (IPETA (TA))
Bouzidi Laurent (IPETA (TA))

• **CHEM & IHEDN**

Auditeurs sélectionnés :

Wencker Michel (ICA), CHEM & IHEDN
Bruni Eric (IG2A), IHEDN



**LEADER MONDIAL
DES SYSTÈMES
DE COMMANDEMENT ET
DE CONTRÔLE, DES
RADARS DE DÉFENSE
AÉRIENNE ET DES
RADARS DE
CONTRE-BATTERIE**

www.thalesraytheon.com

**RENDEZ-NOUS
VISITE À EURSATORY 2010
STAND THALES #A510
STAND RAYTHEON #M102**

Lu au JO

• **1^{er} janvier 2010 : Décret du 31 décembre 2009 portant affectation d'officiers généraux**

Le décret porte nouvelle nomination dans les postes de direction de la Direction générale de l'armement après sa réorganisation du 5 octobre 2010.

• **1^{er} janvier 2010 : Décret n° 2009-1790 du 31 décembre 2009 modifiant plusieurs décrets fixant les indices de solde applicables à certains militaires**

Le décret 2009-1790 modifie, entre autres, les indices des grades et échelons des corps des ingénieurs de l'armement précédemment fixés par le décret 2009-18 du 7 janvier 2009.

• **5 janvier 2010 : Arrêté du 31 décembre 2009 portant nomination au conseil d'administration de l'Institut des hautes études de défense nationale**

Sont nommés membres du conseil d'administration de l'Institut des hautes études de défense nationale, à compter du 1er janvier 2010, sur proposition du ministre chargé de la fonction publique, en qualité de représentant des associations d'auditeurs, M. Bernard Besson, président de l'association des auditeurs du Centre des hautes études de l'armement, et, sur proposition du ministre de la défense, en qualité de représentant de l'Etat, M. l'ingénieur général de l'armement Patrick Auroy.

• **17 janvier 2010 : Décret du 15 janvier 2010 portant nomination d'un directeur adjoint à l'Institut des hautes études de défense nationale (Premier Ministre)**

Est nommé directeur adjoint à l'Institut des hautes études de défense nationale, l'ingénieur général de 1^{ère} classe de l'armement Robert Ranquet.

• **26 janvier 2010 : Décret du 25 janvier 2010 portant nomination au conseil d'administration du Centre national d'études spatiales**

Est nommé membre du conseil d'administration du Centre national d'études spatiales, en qualité de représentant de l'Etat désigné par le ministre de la défense M. Patrick Auroy.

• **28 janvier 2010 : Décret du 26 janvier portant promotions et nominations**

Sont promus au grade d'ingénieur général de 1^{ère} classe, les ingénieurs généraux de 2^e classe Jean Douat, et Thierry Duquesne

(1/03/2010). Sont nommés au grade d'ingénieur général de 2^e classe, les ingénieurs en chef Didier Massonnet, Lionel Suchet, Yves Chevalier et Laurent Sellier (1/03/2010).

• **9 février 2010 : Décret du 8 février 2010 portant nomination du président du conseil d'administration de l'économat de l'armée**

Est nommé président du conseil d'administration de l'économat de l'armée M. Louis Defline.

• **21 février 2010 : Décret du 19 février portant promotions et nomination**

Est nommé inspecteur de l'armement pour l'aéronautique et l'espace, et se voit conférer les rang et appellation d'ingénieur général hors classe de l'armement à compter du 8 mars 2010, l'ingénieur général de 1^{ère} classe de l'armement Philippe Caplain. Sont nommés au grade d'ingénieur général de 2^e classe, les ingénieurs en chef Philippe Wolf, José Godin, Jérôme Pénicaud et François Demoulin (1/04/2010).

• **7 mars 2010 : Décret du 5 mars 2010 portant affectation d'officiers généraux**

Est nommé inspecteur de l'armement, chef de l'inspection, et maintenu dans ses fonctions d'inspecteur de l'armement pour les constructions navales, à compter du 8 mars 2010, l'ingénieur général hors classe de l'armement Patrick Renvoisé.

Est nommé président de la section carrières du Conseil général de l'armement, à compter du 1^{er} avril 2010, l'ingénieur général de 1^{ère} classe de l'armement Alain Costes.

Est chargé de la sous-direction "Europe - Amérique du Sud" du Service du soutien aux exportations de défense de la Direction du développement international, à compter du 1^{er} avril 2010, l'ingénieur général de 1^{ère} classe de l'armement Pierre Lusseyran.

Est chargé des fonctions de directeur adjoint des plans, des programmes et du budget, à compter du 8 mars 2010, l'ingénieur général de 1^{ère} classe de l'armement Henri Cornet.

Est chargée de la sous-direction des sites et de l'environnement du Service central de la modernisation et de la qualité, à compter du 8 mars 2010, l'ingénieur général de 2^e classe de l'armement Marie-France Legrand épouse t'Kint de Roodenbeke.

Est nommé co-vice-président national du bureau des C3 de l'Organisation du traité de l'Atlantique Nord, à compter du 1^{er} mars 2010, l'ingénieur général de 2^e classe de l'armement Patrick Fermier.

• **11 mars 2010 : Arrêté du 1^{er} mars 2010 portant désignation du vice-président du Conseil général de l'armement**

M. Jean-Paul Herteman est nommé, pour une durée de trois ans, vice-président du Conseil général de l'armement.

• **20 mars 2010 : Décret du 18 mars 2010 portant affectation d'officiers généraux**

Est nommé chargé de mission affaires stratégiques et espace auprès du délégué général pour l'armement, à compter du 1^{er} avril 2010, l'ingénieur général de 1^{ère} classe de l'armement Pierre-André Roth.

Est nommé directeur du Centre d'achèvement et d'essais des propulseurs et engins de la Direction technique, à compter du 1^{er} avril 2010, l'ingénieur général de 1^{ère} classe de l'armement Jean-Luc Masset.

Est nommé directeur de DGA Essais en vol à la Direction technique, à compter du 1^{er} avril 2010, l'ingénieur général de 2^e classe de l'armement Jean-Eric Chevillot.

• **30 mars 2010 : Arrêté du 29 mars 2010 portant cessation de fonctions et nomination à la présidence de la République**

Est nommé conseiller technique à la présidence de la République M. Benjamin Gallezot.

• **2 avril 2010 : Arrêté du 29 mars 2010 portant cessation de fonctions et nomination au cabinet du ministre**

Est nommé conseiller pour les affaires industrielles au cabinet du ministre, l'ingénieur en chef de l'armement Pascal Chauve.

• **3 avril 2010 : Décret du 1^{er} avril 2010 portant affectation d'un officier général**

Est nommé chargé de mission auprès du président de la section carrière du Conseil général de l'armement, à compter du 12 avril 2010, l'ingénieur général de 2^e classe de l'armement Jean-Marie Durand.

• **13 avril 2010 : Arrêté du 30 mars 2010 portant nomination au conseil d'administration de l'Ecole nationale supérieure des ingénieurs des études et techniques de l'armement**

Est nommé membre du conseil d'administration de l'Ecole nationale supérieure des ingénieurs des études et techniques de l'armement, en qualité d'inspecteur de l'armement pour les

Carnet professionnel

Louis Defline (1942) a été nommé Président du conseil d'administration au sein de Economat des armées (15/02/2010)

Yves Buey (1962) a été nommé Conseiller auprès du DG (M. Frédéric VAN ROEKEGHEM) pour les questions d'informatique au sein de CNAMTS (23/02/2010)

Alain Costes (1955) a été nommé Pdt de la section carrières au sein de Min de la Défense/CGARM (01/04/2010)

Philippe Logak (1968) a été nommé Secrétaire général au sein de SFR (ex Groupe CEGETEL)/ La Défense - Siège (01/03/2010)

Philippe Lugherini (1958) devient PDG de la société CILAS, filiale d'EADS et AREVA. Il conserve jusqu'en décembre la présidence de Nuclétudes, qu'il dirigeait depuis 2005. (12/03/2010)

Jean-Marie Durand (1958) a été nommé Chargé de mission auprès du président de la section Carrières du Conseil Général de l'Armement (12/04/2010)

Robert Ranquet (1953) a été nommé Directeur Adjt au sein de l'IHEDN (16/02/2010).

Jean-Marie Veys (1955) a été nommé Délégué régional adjoint à la recherche et à la technologie au sein de Institut National Polytechnique de Toulouse (01/03/2010)

Benjamin Gallezot (1972) a été nommé Conseiller technique au sein de Présidence de la République/Cabinet (29/03/2010)

Gautier Roux (1983) a été affecté Base de l'Aéronautique Navale de landivisiau au sein de l'EMM (01/04/2010)

Romain Berline (1974) a été nommé Expert national détaché à Bruxelles (Belgique) au sein de Commission Européenne (16/04/2010)

constructions navales et sécurité nucléaire, l'ingénieur général de l'armement Paul Denais.

• 2 mai 2010 : Arrêté du 28 avril 2010 fixant le nombre de places offertes au recrutement en 2010 dans les corps des ingénieurs de l'armement et des ingénieurs des études et techniques de l'armement

Le nombre de places offertes pour le recrutement d'ingénieurs de l'armement en 2010 est fixé à :

- 18 places au titre du tableau de classement de sortie de l'Ecole Polytechnique (article 4 du décret 2008-941)

- 3 places au titre du recrutement en cours de carrière par concours sur épreuves au grade d'ingénieur de l'armement (article 6 - 1°)

- 3 places au titre du recrutement en cours de carrière par concours sur épreuves au grade d'ingénieur principal de l'armement (article 6 - 2°).

18 mai 2010 : Arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité : le référentiel général de sécurité (disponible sur www.ssi.gouv.fr/rgs), qui fixe les règles de développement de procédures et transactions en ligne sécurisées, favorise

la conception et la mise en œuvre par les administrations de téléservices fiables et protégés. Applicable à l'ensemble des autorités administratives françaises (état, collectivités territoriales, établissements publics administratifs et de protection sociale...), il permettra d'accélérer l'administration en ligne et la dématérialisation des procédures administratives dans des conditions de sécurité adaptées, favorables à la confiance des usagers des services publics.

Daniel Jouan, IGA

MASTER IN STRATEGY



12345678901234567890
12345678901234567890
12345678901234567890

12345678901234567890
12345678901234567890

12345678901234567890
12345678901234567890

12345678901234567890

329849

347728

defense aerospace and security systems



high-tech **initiation** company

B.D.S.A. Le Herre - 12/2006 - RCS 315 437 567 00054
Photo credités : eMAGIA - Sergez Au - Sergez Bern

 **davey bickford**

**Le Moulin Gaspard
89550 Héry - France**

Sales : tel +33 (0)3 86 47 30 53

tel +33 (0)3 86 47 30 30

Fax : +33 (0)3 86 47 94 04

def.aero@daveybickford.fr

www.daveybickford.com

Mobilité et efficacité sur tous les terrains

- Carcasses haute longévité
- Utilisation mixte
- Capacité de franchissement élevée
- Maîtrise des coûts



www.continental.fr

Continental 
Tires - Engineered in Germany