ADA N° 365
NOVEMBRE - DÉCEMBRE 2011
www.defense.gouv.fr

ARMÉES D'AUJOURD'HUI

M 01139 - 365 - F: 3,00 € - RD

DOSSIER

CYBERESPACE

LE 5eme CHAMP DE BATAILLE

ARMÉES D'AUJOURD'HUI

Sommaire

N° 365

4 FORCES EN ACTION

Livraison par air échange franco-belge

Les militaires des deux pays se sont retrouvés dans le Sud de la France pour partager leurs expériences dans le domaine de la livraison par air. Au menu : largages de matériel et de personnel et échanges humains.

32 DOSSIER

Cyberespace, le 5e champ de bataille

L'équilibre des Etats repose sur les systèmes d'information. La Défense n'y échappe pas. Des moyens radios aux messageries internes, des systèmes d'armes aux téléphones portables, le numérique est devenu l'incontournable outil de travail... et parfois vulnérable.

58 DÉTOURS CULTURE

BSPP : deux siècles dans le feu de l'action

Créée par Napoléon en 1811, la brigade de sapeurs-pompiers de Paris fête son bicentenaire. Sa mission : protéger les personnes et les biens. Sa devise : Sauver ou périr.

ARMÉES D'AUJOURD'HUI. **Directeur de la publication :** Dicod. **Directeur de la rédaction :** colonel (terre) Benoît Trochu. **Chef du bureau de la rédaction :** lieutenant-colonel (air) Bruno Cunat. **Rédacteur en chef :** lieutenant-colonel (terre) Philippe Dupas. **Rédacteur en chef adjoint :** capitaine (terre) Anne-Lise Llouquet (01 44 42 48 01). **Conception graphique :** Olivier Spadaccini. **Secrétariat de rédaction :** Juliette Démoutiez, Yves Le Guludec. **Chef des reportages :** sergent-chef (terre) Alban Vasse (48 02). **Rédaction :** enseigne de vaisseau Grégoire Chaumeil (40 04), aspirant (marine) Barthélemy Gruot (45 83), Paul Hessenbruch (55 05), Eléonore Krempff (44 35), Samantha Lille (47 27), Nelly Moussu (46 29). **Prestations intellectuelles :** enseigne de vaisseau Cynthia Glock, lieutenant de vaisseau Christelle Haar, Jean-Claude Jaeger, Pierre Journoud, Rouge Vif (Domitille Bertrand, Stéphane Tudela). **Service photo :** adjudant-chef (air) Bruno Biasutto (47 44), CCH (terre) Jean-Jacques Chatard (46 98). **Service icono :** Christophe Deyres (48 35), Carole Vennin (45 09). **Chef de fabrication :** Thierry Lepsch : 01 44 42 32 42. **Photogravure :** Open Graphic Media. **Impression et mise en page :** Bedi Sipap. **Routage :** CRP. Commission paritaire n° 0211 B 05686. **Dépôt légal :** février 2003. Dicod – Ecole militaire – 1, place Joffre – 75007 Paris.

Abonnement payant (ECPAD) : 01 49 60 52 44. routage-abonnement@ecpad.fr.

Diffusion - abonnement gratuit : sergent-chef (air) Céline Butaud : 01 44 42 40 07. celine.butaud@dicod.defense.gouv.fr

Contact publicité (ECPAD) : Christelle Touzet : 01 49 60 58 56 / regie-publicitaire@ecpad.fr

Photo de couverture : © Photodisc

Livraison par air
Echange franco-belge dans le ciel

Les spécialistes français du 35e Régiment d'artillerie parachutiste embarquent à bord de l'Hercules de l'armée belge.

Du 28 septembre au 3 octobre, militaires belges et français se sont retrouvés dans le sud de la France pour partager leurs expériences dans le domaine de la livraison par air. Au menu : largages de matériel et de personnel accompagnés, bien sûr, d'un très riche échange humain.

Par Samantha Lille / Photos : Jean-Jacques Chatard / DICOD


gascon

« Même si leur matériel et leurs procédures sont américains, l'organisation des Belges est très proche de la nôtre. »

Ci-dessus à gauche : Le lieutenant Trenson, des forces belges, vérifie l'équipement des parachutistes français qui vont sauter. Chaque sangle doit être correctement fixée pour ne pas vriller.
Ci-dessus à droite : En file indienne, à l'approche de la zone de saut, Français et Belges accrochent leur sangle d'ouverture automatique.
Ci-contre : Des chuteurs des deux nations s'élancent de l'avion à 3 000 m d'altitude.
Ci-dessous, de gauche à droite : Des hommes de la BOAP préparent une jeep sous la tente gonflable du chantier mobile de conditionnement. Une fois en l'air, la charge est extraite par un parachute éjecteur belge. A l'atterrissage, les cartons jouent leur rôle d'amortisseurs et s'écrasent à l'impact. La Jeep est prête à être utilisée.

Rassemblés sur un talus de l'aéroport de Tarbes, neuf militaires du 35e régiment d'artillerie parachutiste enfilent leurs casques lourds. En file, ils suivent les instructions du lieutenant Patrick Trenson, commandant le peloton de ravitaillement par air (RavAir) belge. *« Vous m'appelez quand vous avez mis en place le dorsal »*, crie l'officier. Quart de tour sur la gauche, un pas en avant et sangle d'ouverture automatique (SOA) levée dans la main droite, tous se présentent équipés. Ils s'apprêtent à sauter pour la première fois avec le parachute qui équipe l'armée belge. Ces hommes et ces femmes participent à l'exercice de livraison par air franco-belge Pegase 3, organisé par la 11e brigade parachutiste. L'occasion pour ces acteurs de l'armée de terre et de l'armée de l'air des deux nations de travailler leur savoir-faire en assurant des reconductions de qualifications. *« Nous nous sommes déjà retrouvés sur des théâtres africains ensemble. Nous avons une convergence dans nos modes de travail et de pensées. S'entraîner en binational, c'est une manière de préparer l'arrivée de l'A400M, un avion de transport que nos deux pays vont recevoir, avec en tête l'idée de développer un système de livraison par air commun et une standardisation du matériel et des procédures »,* explique le colonel Fauche, chef de corps du 1er Régiment du train parachutiste (RTP) qui lui aussi se prépare. Il fera partie du vol, en temps que chuteur.

Au sein du groupe, un homme se détache. L'adjudant-chef Lamouroux, instructeur au 1er RTP, vérifie lui aussi les équipements des hommes qui s'apprêtent à partir : chaque sangle doit être bien fixée et ne pas vriller. Un peu plus tôt dans la journée, il a mené une instruction d'une trentaine de minutes pour leur présenter ce matériel. *« Cet échange permet d'éduquer nos jeunes sur de nouvelles techniques,* explique-t-il. *Nous allons bientôt percevoir l'EPC (ensemble du parachutage du combattant), très proche du parachute utilisé par les Belges, avec une voile plus grande et orientable. »*

Au même moment, à quelques mètres de là, une équipe décharge une jeep d'un camion. Elle sera embarquée dans l'Hercules belge, fourni par le Commandement européen du transport aérien militaire (EATC). Hommes et matériel seront largués à partir du même avion. Dans l'appareil, les hommes du peloton RavAir placent les taquets d'arrimage afin de fixer l'imposant colis. Le véhicule arrive de la base opérationnelle aéroportée (BOAP) située à une quinzaine de kilomètres de là, sur le camp de Ger, où il a été conditionné. Déployée pour l'exercice, la BOAP met en œuvre un chantier mobile de conditionnement et de transit qui comporte une tente gonflable de 60 mètres de long. C'est à l'intérieur de celle-ci que les équipes réceptionnent le matériel et le mettent en forme grâce à des chemins de roulement au sol et une plate-forme élévatrice. *« Même si leur matériel et leurs procédures sont américaines, l'organisation des Belges est très proche de la nôtre »*, résume le commandant Carrasquedo, chef de la BOAP. Les colis seront ensuite prêts à être largués et opérationnels dès leur atterrissage.

A l'aéroport, au pied de l'appareil, le commandant Jorissen relit sa feuille de vol. Pour cet officier, collaborer avec les Français n'est pas une première. En 2010, il avait déjà participé à un exercice similaire à Pau. *« On peut y aller »*, lance-t-il à son compatriote chef largueur. D'un signe de la main, celui-ci indique aux parachutistes qu'ils peuvent embarquer.

Une fois en l'air, les petits rires nerveux s'effacent pour laisser place au silence et à la concentration. Dix minutes après le décollage, la tranche arrière s'ouvre à 300 mètres du sol. Debout, largueurs et mécaniciens navigants se placent de chaque côté de la charge. Un échange de regards, un geste, un claquement bref et la Jeep est littéralement happée. *« Le largage par éjection consiste à utiliser un parachute éjecteur pour extraire la charge de l'avion, c'est une procédure utilisée pour la mise à terre d'engins lourds et encombrants »,* explique le capitaine Talluault, chef du secteur Livraison par air sur la BOAP.

Au sol, les cartons amortisseurs remplissent leur rôle et s'écrasent, découvrant le véhicule : intact. Dans l'Hercules, le lieutenant Trenson lance le décompte : le 35e RAP sautera dans dix minutes, en ouverture automatique en tranche arrière. *« Get Ready ! »* Tous s'avancent, accrochent leur SOA au câble de l'avion. Face à la colonne, l'instructeur esquisse un mouvement semblable à un pas de deux. Contrairement à leur habitude, les parachutistes français vont devoir sauter bras tendus le long du corps et non joints sur les épaules. Le commandant de bord donne le signal, le chef largueur fait signe au premier Français d'y aller. Dans le ciel, neuf voiles vertes de 100 m² s'ouvrent. Sur la zone de saut, ils ont à peine le temps de se poser que les commentaires fusent : *« Une voile orientable ça change tout », « Des sauts comme celui-là, on veut bien en faire quatre par jour ».*

Derniers à entrer en piste, les chuteurs. Belges et Français vont sauter ensemble. La tranche arrière s'ouvre une troisième et dernière fois. Cette fois-ci, ce ne sont plus les champs de maïs et les habitations qui défilent mais un ciel bleu dégagé : l'avion vole à 10 000 pieds soit 3 000 mètres. Onze hommes s'élancent avec des voiles rectangulaires aux couleurs de la France et de la Belgique avec pour fond les Pyrénées sous un soleil rasant. ■

Centre national d'entraînement commando

L'école des anges gardiens

Des tirs d'artillerie se font entendre, le garde du corps emmène l'autorité à couvert pour la protéger des tirs de mortier et procèder dès que possible à son évacuation.

Avant chaque déploiement sur un théâtre, les hommes choisis pour faire partie du détachement d'accompagnement d'autorité passent par le centre national d'entraînement commando. Vingt jours de formation pour se familiariser avec le monde de la garde rapprochée et consolider leurs capacités d'autonomie, de réactivité et de sang-froid.

Par Samantha Lille / Photos : Jean-Jacques Chatard / DICOD

« Ici, nous leur donnons des bases, à eux de continuer à s'entraîner et de développer un esprit d'équipe. »

Ci-dessus : Les stagiaires du CNEC mettent en pratique la formation acquise durant deux semaines. Ils doivent escorter une autorité dans un environnement rendu hostile.

Ci-contre : Les stagiaires prennent contact avec l'autorité et lui donnent quelques consignes de sécurité.

Trois véhicules escortant une autorité militaire arrivent au niveau d'un check point. Après plusieurs minutes de discussions, le convoi se remet en route et s'apprête à franchir la barrière quand un *« suicide bomber »* se fait exploser à quelques mètres de la première voiture. Immédiatement, les véhicules font marche arrière mais un tireur embusqué ouvre le feu. *« Contact à gauche »*. L'autorité est évacuée mais la voiture suiveuse est immobilisée. Les quatre occupants ripostent *« Carmin ici Diego, parlez ! »* La liaison radio ne reviendra pas.

Ces hommes en action participent à l'exercice de synthèse du stage détachement d'accompagnement d'autorité (DAA) créé par le centre national d'entraînement commando (CNEC). Conçue en 2005, cette formation de trois semaines est destinée à des unités de l'armée de terre en partance pour un théâtre. Elle fait partie intégrante de leur mise en condition avant projection. Les régiments désignent une dizaine d'éléments triés sur le volet dont la plupart sont issus des sections d'aide à l'engagement débarqué (SAED). Sur le territoire, ils vont accompagner et protéger un chef de corps, représentant français, général ou VIP de passage. Pendant trois jours à Collioure (Pyrénées-Orientales), ils doivent escorter une autorité militaire lors de divers déplacements dans un environnement rendu hostile. *« Cette synthèse est la restitution du savoir-faire qu'ils ont appris pendant les deux premières semaines d'instruction : procédures de débarquement et d'embarquement de véhicules, fouilles de bâtiment, élaboration de fiches d'itinéraire et de dossiers de sites, tirs avec arme de point, d'épaule et fusil mitrailleur »,* résume l'adjudant L., instructeur au CNEC.

Mise en situation

De retour au Fort Miradou de Collioure, les stagiaires entrent en salle. Face à eux, les instructeurs font part de leurs remarques : *« Attention au délai. Vous aviez quinze minutes d'avance pour le rendez-vous. C'est trop »*, insiste l'adjudant M. Egalement présent, le lieutenant-colonel Leheu, directeur général de la formation et VIP du jour. *« Il y a des décisions difficiles à prendre, comme partir et laisser des hommes sur le terrain. Mais votre mission reste la sécurité de l'autorité ».*

Le détachement n'a pas le temps de souffler. Ce soir, l'homme qu'ils protègent doit dîner en ville avec d'importantes personnalités. Pour préparer ce rendez-vous au sommet, ces militaires vont reconnaître les différents itinéraires possibles, le site et faire un point sur les menaces particulières. A 20 h 45, le convoi prend la route. Une fois sur place le dispositif s'active : « Etoile » – le nom de code du VIP – s'installe avec ses interlocuteurs. Deux hommes de sa protection rapprochée s'attablent à quelques mètres. L'autorité ne doit jamais rester seule. A l'extérieur, les conducteurs sont en alerte. Quatre militaires patrouillent aux abords de l'établissement. L'attente va être très longue, pourtant à aucun moment leur vigilance ne baissera. Sur le chemin du retour, un pneu du véhicule d' « Etoile » crève. Celle-ci est aussitôt transférée dans la voiture de tête par « l'homme d'épaule », son garde du corps personnel.

Une fois tous les acteurs rentrés, les différentes phases du scénario sont analysées. *« Tu as pris un prospectus provenant d'un inconnu. Aujourd'hui, il y avait de la colle dessus mais ça aurait pu être un agent bactériologique »,* fait remarquer un des instructeurs à un stagiaire. Tous les types de menaces sont pris en compte. *« Il vaut mieux qu'ils fassent un maximum d'erreurs ici plutôt que sur le théâtre,* ajoute-il. *Nous leur donnons des bases, à eux de continuer à s'entraîner et de développer un esprit d'équipe, primordial sur le terrain ».*

Le lendemain matin, l'autorité doit s'entretenir avec un chef militaire au fort Bear, à Port-Vendres. Des manifestations sont à craindre dans la ville mais le VIP insiste, cette rencontre est capitale. *« Souvent, le plus difficile est d'alerter l'autorité sur les risques qu'elle encourt quand celle-ci tient absolument à réaliser sa mission »*, souligne le lieutenant-colonel Leheu. Etre calme, autonome, réactif et savoir anticiper, autant de qualités que chaque homme de cette garde rapprochée doit posséder.

« Ici Protec, on amorce la montée », annonce le sous-officier. Le véhicule porteur – celui avec l'autorité – passe en tête. *« Regardez sur la tour, je crois qu'il y a des hommes armés. »* Arrivé sur place, le DAA forme une véritable bulle de protection autour de l'autorité. La rencontre ne va pas se passer comme prévu. *« Ici John, problème pendant le rendez-vous, on descend. »* Le garde du corps finit à peine sa phrase qu'une détonation se fait entendre. *« Artillerie ! »* hurle un des hommes du détachement. Tête baissée, le colonel est emmené dans un tunnel pour être protégé des tirs de mortier. Quelques minutes s'écoulent. *« Tir terminé. On évacue, on descend au véhicule. »* En courant, le petit groupe s'engouffre dans une voiture. Le démarrage est brutal. Au même moment, les manifestations à Port-Vendres prennent de l'ampleur. Décision est prise d'évacuer le VIP par voie nautique pour éviter qu'il ne reste immobilisé en ville. *« On est sur la plage de Mailly. On vous attend pour l'exfiltration »*, lance le chef du détachement du 3ème RIMa. Quelques minutes plus tard un Zeppelin rapide accoste, les hommes embarquent. La mission est réussie, l'autorité est rentrée saine et sauve. ■

Soixante-six ans après la fin de la Seconde Guerre mondiale, une découverte d'engin non explosé est signalée tous les trois jours en moyenne au centre des opérations de la marine de Cherbourg. Le groupe de plongeurs démineurs entre alors en scène.

Par Christelle Haar (préfecture maritime de Cherbourg)/Photos : F. Duplouich (marine nationale)

Plages normandes
Dépollution à haut

risque

« Vu l'environnement, seuls les plongeurs démineurs de la marine sont capables d'assurer ce chantier. »

Les plongeurs démineurs (la marine nationale en compte 3 groupes) interviennent sur tout type de munitions conventionnelles ou non, tant en milieu terrestre que subaquatique. Ils mènent également des travaux sous-marins en tout genre et sont amenés à être projetés sur les théâtres d'opérations extérieures aux cotés de leurs homologues démineurs des autres armées.

Octobre 2011, 10 heures. Le chef de mission du Groupe des plongeurs démineurs (GPD) de la Manche*, le maître Emmanuel Doche, et ses six hommes, s'apprêtent à descendre en rappel une falaise de plus de 30 mètres. A la mairie d'Englesqueville-la-Percée (Calvados), charmante et tranquille bourgade normande de 70 âmes, c'est l'effervescence. Toute cette semaine, le village, d'habitude si tranquille, va être le théâtre d'une importante opération de déminage.

Plusieurs centaines de munitions de toutes natures et de tous gabarits ont été découvertes au pied d'une falaise de ce petit village situé à quelques kilomètres de la pointe du Hoc. *« Dans la précipitation de l'après-guerre, il a sans doute été décidé de se débarrasser des restes de munitions à cet endroit car il était difficilement accessible »,* explique Jacques Ranchère, sous-préfet de Bayeux, responsable du PC installé pour l'occasion à la mairie. Même difficilement accessibles et officiellement interdites par deux arrêtés préfectoraux, les plages attirent les curieux et les collectionneurs du fait de la densité des munitions encore présentes. *« Il était indispensable de réaliser ce chantier, malgré les nuisances qu'il allait occasionner sur la vie locale. Vu l'environnement, seuls les plongeurs démineurs de la marine nationale étaient capables d'assurer cette mission, à mi-chemin entre terre et mer. C'est pour cette raison que le préfet du Calvados a fait appel à la marine nationale »*, complète le sous-préfet.

Opération parfaitement planifiée

Pour tenir compte des impacts environnementaux (le chantier est situé dans une zone Natura 2000), l'opération a été programmée à l'automne, afin de ne pas nuire à l'évolution de certaines espèces d'oiseaux. Début septembre, le maître Doche a exposé à la population le déroulement du chantier de dépollution. Celui-ci se déroulera en deux phases : la première consistera à regrouper dans des fûts les munitions déplaçables, à les transporter à distance raisonnable en mer pour les pétarder au loin et ainsi diminuer les effets sur la population. Le maître Doche estime pouvoir traiter la plus grosse part des munitions de cette façon. La deuxième phase concernera les munitions qui ne peuvent être déplacées. Le temps ayant fait son travail, de nombreuses munitions sont en effet enchâssées dans les rochers. Il faudra les relier une par une et les traiter par un pétardement terrestre. Evidemment, lors de cette phase, les distances de sécurité nécessiteront des évacuations de population. C'est le sujet délicat. *« La sécurité de vos enfants nécessitera de quitter votre logement deux demi-journées »,* appuie le sous-préfet. Tout le monde s'implique : les gendarmes de la brigade pour le blocage des routes, les autocaristes pour revoir l'organisation du ramassage scolaire, etc. 3 octobre, 10 h 50. Toute l'équipe est au pied de la falaise. Les choses se déroulent conformément à la planification. L'équipe délimite un périmètre d'intervention : 200 mètres de long sur 50 de large. Au PC, en mairie, l'officier opérations du GPD Manche, le lieutenant de vaisseau Yann Geffroy, prend ses marques. C'est lui qui, aux côtés du sous-préfet, donnera le « vert » pour les pétardages. Sur la plage, durant toute la journée, la collecte s'effectue : près de 1 200 projectiles d'artillerie sont ramassés, déplacés avec soin, triés avec précision. Une « prise » énorme !

Intervention efficace et rapide

Mardi 4 et mercredi 5, les plongeurs, grâce au concours de la *Magnolia*, leur vedette d'intervention, et sous la surveillance de la vedette de gendarmerie maritime *Yser*, déplacent plus de 800 munitions en mer et les traitent à 3 kilomètres du rivage, sous 10 mètres d'eau.

La difficulté réside dans la réaction des riverains pour les journées de jeudi et de vendredi. La plupart des habitants sont agriculteurs et éleveurs. L'heure de la traite des vaches ne correspond pas à celle de la marée et donc pas à celle de l'évacuation. Les plongeurs démineurs essaient de limiter au minimum leur délai d'intervention. Les échanges se passent bien et les contraintes sont comprises par tous. En deux jours, 400 munitions sont traitées à terre ! Le pétardement du premier jour ayant révélé de nouvelles munitions cachées sous les rochers.

Vendredi à 15 h 30, le chantier est terminé. Le lieutenant de vaisseau Geffroy et le maître Doche annoncent… 1 202 munitions traitées. Madame le maire pousse un *« ouf »* de soulagement. La bourgade va pouvoir reprendre son rythme habituel.

Pour les marins du GPD Manche, c'est une belle expérience, un chantier original qui s'ajoute à ceux générés par les quelques 300 engins traités chaque année sur les 7 départements côtiers de la façade maritime de la Manche et mer du Nord. ■

Christelle Haar

* Chaque GPD a une fonction bien définie : le GPD Manche est spécialisé dans le contre terrorisme maritime (dépiégeage d'assaut), le GPD Atlantique intervient dans des eaux polluées et est expert en engins inconnus, le GPD Méditerranée est acteur dans les opérations amphibies.

PAR BARTHÉLEMY GRUOT

19/10 AFGHANISTAN : PREMIER DÉSENGAGEMENT

G. MARIETTE/ECPAD

Le 19 octobre, un premier contingent d'un peu moins de 200 militaires français a été désengagé d'Afghanistan. Il s'agissait principalement d'une compagnie de combat et de ses appuis déployés à Tora, en Surobi, au nord-est de Kaboul. Elle était armée par le 2e Régiment étranger de parachutistes, le 35e Régiment d'artillerie parachutiste et le 17e Régiment du génie parachutiste. Ce retrait atteste des progrès opérationnels accomplis par les soldats afghans, accompagnés par l'armée française depuis 2008, mais également de l'amélioration de la situation sécuritaire en Surobi. Au total, près de 3 800 militaires français demeurent en Afghanistan, dont 450 en Surobi. Ils effectuent des missions de soutien au profit des forces afghanes pour la sécurisation des régions (Surobi et Kapisa) et participent aux actions de formation, principalement sur Kaboul.

1-3/10 LIBYE : LE « TONNERRE » ACCUEILLE UN DÉTACHEMENT AMÉRICAIN

Du 1er au 3 octobre 2011, un détachement *Personal Recovery* (PR) de la coalition, armé par des hélicoptères HH60G Pave Hawk a été accueilli sur le bâtiment de projection et de commandement (BPC) *Tonnerre*. Le but étant de valider, au plus près des côtes, la capacité du BPC à recevoir un détachement *Combat Search and Rescue* (CSAR) supplémentaire, pour renforcer ponctuellement cette capacité. La mission sur le *Tonnerre* a été l'occasion de nombreux échanges. Et les militaires américains se sont dits impressionnés par la configuration du BPC et la capacité d'accueil de son hangar hélicoptères. ...

P. SOLA/MARINE NATIONALE/EMA

06/10 LIBAN : RELÈVE À LA FORCE COMMANDER RESERVE

C'est le colonel Cédric du Gardin, chef de corps du 1er Régiment de tirailleurs d'Epinal, qui a pris la succession du colonel Renaud de l'Estoile, du 1er Régiment de chasseurs à Verdun, à la tête de la *Force Commander Reserve* (FCR). Directement placée sous les ordres du commandant de la Force intérimaire des Nations unies au Liban (Finul), la FCR agit dans le cadre de la résolution 1701 de l'ONU. Elle compte près de 850 militaires et dispose de moyens uniques sur le théâtre, notamment, en matière de veille radar ou d'appuis feu.

04/11 CÔTE-D'IVOIRE : RETOUR DU DETALAT LICORNE EN FRANCE

Après neuf années de présence sur ce territoire, le détachement de l'aviation légère de l'armée de terre (Detalat) a quitté la Côte-d'Ivoire. Ce départ intervient dans un contexte de normalisation de la situation sécuritaire du pays. Il constitue la première étape du passage de la force Licorne à un effectif d'environ 450 militaires, avant les élections législatives du 11 décembre. Cependant, les forces françaises conservent une capacité aéromobile avec la présence d'un hélicoptère Fennec de l'armée de l'air et la possibilité d'accueillir des renforts de l'Alat basées en Afrique et en France.

29/10 LA RÉUNION : LES MILITAIRES FRANÇAIS ENGAGENT DES MOYENS IMPORTANTS POUR LUTTER CONTRE L'INCENDIE DU PARC NATIONAL

Près de 500 militaires des trois armées (terre, air, marine) et de la sécurité civile ont contribué à lutter contre l'incendie de grande ampleur qui s'est déclaré dans le parc national de l'île de La Réunion.
Une trentaine de volontaires du régiment du service militaire adapté (RSMA) et une trentaine de parachutistes du 2e régiment de parachutistes d'infanterie de marine (2eRPIMa) ont nettoyé le terrain pour éviter la progression du feu.

RICHARD BOUHET/AFP

Puis les forces armées de la zone sud de l'océan Indien (Fazsoi) ont engagé une centaine d'hommes, une dizaine de poids lourds, des bus et une quinzaine de véhicules tout-terrain.
Le 29 octobre, face à l'aggravation de la situation, 350 militaires de la sécurité civile et environ 20 tonnes de fret ont été acheminés depuis la métropole.
Les Fazsoi avaient déjà été engagés en octobre 2010 sur un incendie à La Réunion et ils avaient déployé plus de 130 militaires.

31/10 LIBYE : FIN DE L'OPÉRATION UNIFIED PROTECTOR DE L'OTAN

Les moyens militaires engagés par la France dans les opérations en Libye sont officiellement désengagés de l'opération *Unified protector*. Les moyens qui étaient encore déployés fin octobre sur zone (3 Mirage 2000D à La Sude en Grèce, 5 Rafale et un drone à Sigonella en Italie, un bâtiment aviso, le *commandant Birot*) ont terminé leurs missions au profit de l'Otan.
L'alerte des moyens stationnés France est levée.

Cette alerte concernait une force navale (la TF 473, avec son état-major, un BPC, un groupe aéromobile, un plot CSAR, deux frégates et un bâtiment de soutien) et un détachement chasse (une quinzaine de Mirage 2000D, 2000N et F1).

Parallèlement, l'opération Harmattan continue. Elle durera le temps de la manœuvre logistique pour rapatrier les matériels et moyens militaires français encore déployés sur zone.

14/11 AFGHANISTAN : UN LÉGIONNAIRE TUÉ LORS D'UNE OPÉRATION EN KAPISA

**Le légionnaire de 1re classe Goran Franjkovic, du 2e régiment étranger du génie (2e REG) de Saint-Christol, est mort au combat en Kapisa. Il était engagé en Afghanistan depuis début novembre au sein du GTIA Kapisa armé par le *Battle Group Tiger*. C'est au cours d'une opération de sécurisation de l'axe Vermont et d'escorte d'un convoi logistique franco-afghan que l'élément français présent sur cette zone a été pris à partie par des tirs d'insurgés.
Âgé de 25 ans, le légionnaire d'origine serbe a été promu au grade de caporal à titre posthume et fait chevalier de la Légion d'honneur par le ministre de la Défense.
Il est le 76e soldat français mort en Afghanistan.**

SIRPA TERRE

PHOTOS : R. NICOLAS-NELSON/ARMÉE DE L'AIR / SIRPA-AIR

Ci-dessus : Les Alpha-jet de l'escadron 2/2 Côte-d'Or (Dijon) en formation serrée aux côtés des Hawk du 100e escadron de la RAF (Leeming, Grande-Bretagne). A droite : Un débriefing est organisé après chaque mission aérienne, et chacun peut alors exprimer son ressenti.

Dans le cadre de la coopération de défense bilatérale, les acteurs français et britanniques de l'appui aérien se retrouvent pour un entraînement dans des conditions proches de celles rencontrées sur le théâtre afghan. Une répétition générale, du 3 au 14 octobre, qui permet aux deux nations de renforcer leur capacité à être engagées côte à côte.

Epias, une communauté d'action et de langage

Un convoi de ravitaillement de cinq véhicules est attaqué par des insurgés. Immédiatement, un contrôleur aérien avancé français *(Forward Air Controller, FAC)* infiltré au sol signale un TIC *(Troop In Contact :* un accrochage*)* et demande un appui aérien. Une quinzaine de minutes plus tard, un appareil arrive sur zone, il est britannique.

Le tir n'aura pas lieu. Nous sommes à Dijon, à 7 780 km de Kaboul et 760 km de Londres. Soixante militaires français et autant de britanniques se sont réunis sur la base aérienne 102 pour participer à l'Exercice de préparation interarmées et interalliés à l'appui aérien du segment sol, baptisé Epias. Organisé et conduit par le commandement des forces aériennes (CFA) de Metz, il s'étend sur la région du Valdahon (Doubs), de Gray (Haute-Saône) et de Beaune (Côte-d'Or). Côté aérien, des Mirage 2000 D de Nancy, des Rafale de Saint-Dizier, des Alphajet de Dijon, et des avions de chasse d'entraînement Hawk du 100e escadron de la Royal Air Force, déployés pour l'occasion sur la base bourguignonne, se sont partagés le ciel. Au sol, des hommes des trois commandos parachutistes de l'air (CPA 10, 20, 30), ainsi que des équipes de l'armée de terre du 35e régiment d'artillerie parachutiste, 93e régiment d'artillerie de montagne, 68e régiment d'artillerie d'Afrique et 1er régiment d'artillerie de marine, tous encadrés initialement par le centre de formation de l'appui aérien de Nancy, ont guidé les avions aux côtés de leurs homologues britanniques du « RAF régiment ».

« L'objectif de cet exercice est de préparer les forces aériennes et terrestres de nos deux pays à un futur déploiement en Afghanistan. Ensemble, ils peuvent échanger leur expertise et leurs expériences du terrain », explique le lieutenant-colonel Soriano, directeur de l'exercice et chef du bureau Entraînement du CFA. Pour le lieutenant-colonel Gleave, commandant du 100e escadron de la RAF, ces missions conjointes offrent une réelle plus-value : *« Français et Britanniques,*

nous avons bien sûr une longue histoire commune, mais nous partageons surtout un objectif identique : maintenir ensemble notre niveau opérationnel. »

Pendant deux semaines, les engagements vont s'articuler autour de scénarios de missions d'appui aérien rapproché *(Close Air Support, CAS)* mettant en œuvre des personnels insérés dans les structures de commandement, des aviateurs et des troupes au sol impliquant des contrôleurs aériens avancés (forward air controllers). Ces derniers sont chargés de communiquer des informations déterminantes pour la conduite des opérations. Ils doivent coordonner depuis le sol l'action des aéronefs, de l'artillerie et des forces amies présents dans la zone, garantir la précision des frappes et éviter les tirs fratricides et dommages collatéraux. Ce sont eux qui identifient et désignent les objectifs à détruire.

Si les premiers jours ont permis aux participants de prendre contact et de se familiariser avec la culture de chacun, les scénarios des missions se sont complexifiés au fil du temps,

Des actions conjointes franco-britanniques à l'horizon 2015

Partenaires de longue date, les armées françaises et britanniques se connaissent bien. La signature à Londres, le 2 novembre 2010, d'un traité de coopération en matière de défense et de sécurité par le président de la République, Nicolas Sarkozy, et David Cameron, Premier ministre du Royaume-Uni, a permis de concrétiser cette coopération. L'engagement côte à côte en Afghanistan et dans les opérations aéromaritimes en Libye permet d'accélérer la réalisation d'un des objectifs de l'accord de coopération, la constitution d'une « Combined Joint Expeditionary Force » (CJEF). Cette force expéditionnaire devrait entre autres permettre une meilleure capacité franco-britannique à décider et mener des actions conjointes à l'horizon 2015. L'exercice aérien Epias fait ainsi suite à l'exercice franco-britannique Flandres 2011 organisé en juin dernier, qui avait pour objectif d'évaluer l'interopérabilité entre les armées de terre des deux pays et d'identifier les efforts à consentir pour consolider leurs coopérations.

PHOTOS : RICHARD NICOLAS-NELSON / ARMÉE DE L'AIR/SIRPA AIR

« Pour certaines sorties, nous mixons les équipages. Nos sytèmes d'armes ne sont certes pas identiques, mais nous utilisons les mêmes procédures Otan. »

pensés pour être au plus près des schémas afghans. *« Les mêmes règles d'engagement que sur le théâtre sont appliquées ici, nous avons d'ailleurs un conseiller juridique (legad), présent en permanence sur le terrain »,* souligne le directeur de l'exercice.

Si Epias a bien lieu en France, c'est en langue anglaise que pilotes et combattants au sol s'expriment. Ils vont devoir ainsi s'adapter à différents débits de parole et accents, un exercice loin d'être simple et pourtant primordial car dans le combat aérien rapproché, l'à peu près n'a pas sa place. *« Pendant l'exercice,* relate l'adjudant P. du 93e RAM, *lorsque les FAC sont français, nous leur parlons quand même en anglais pour nous habituer car, sur le théâtre, les appareils qui interviennent sont de diverses nationalités. Avoir la possibilité de s'entraîner avec de vrais anglophones, c'est une chance. On se rend compte que certains mots de vocabulaire nous manquent ou que les Britanniques utilisent des expressions bien particulières. Hier, au moment du guidage, nous n'arrivions pas à comprendre que le pilote utilisait un mot d'argot pour nous parler d'un complexe fermier ».* Le lieutenant-colonel Gleave insiste : *« Nos contrôleurs aériens avancés doivent aussi se rendre compte qu'ils ne peuvent pas utiliser un langage ou des abréviations qui n'appartiennent qu'à eux. Il est essentiel qu'ils se fassent comprendre par tous. »*

Les missions aériennes durent environ 90 minutes, elles sont ensuite débriefées avec les deux équipes, air et sol, afin que chacun puisse exprimer ressenti, difficultés ou satisfactions. *« Pour certaines sorties, nous mixons les équipages. On participe à la mission en place arrière du Hawh, on aide à la radio ou on prend les commandes à un moment donné tout en observant les réactions de l'autre. Nos systèmes d'armes ne sont certes pas identiques, mais nous utilisons les mêmes procédures Otan »,* précise le capitaine M., pilote de l'escadron dijonnais, qui a deux séjours en Afghanistan à son actif.

A un mois du départ sur le théâtre de certaines unités participantes, cet exercice d'envergure internationale aura permis aux deux nations de confronter leurs méthodes de travail et surtout de mieux se connaître. Un gage d'efficacité, un impératif opérationnel. ■

Samantha Lille

L'Otan a officiellement mis un terme à l'opération "Unified Protector" le 31 octobre, en lien avec les autorités libyennes et l'ONU. Cette opération, où les forces armées françaises ont joué un rôle majeur, présente notamment une expérience interarmées dont tous les enseignements vont être tirés. L'exemple de la coordination aéro-maritime au large des côtes en témoigne.

Harmattan
interarmées par excellence

Engagés au large des côtes libyennes de mai à octobre 2011 dans le cadre de la Task Force 473 (force aéromaritime), une quinzaine d'hélicoptères de combat et de manœuvre de l'aviation légère de l'armée de terre (Alat) ont embarqué sur le BPC. Pour les marins comme pour les terriens, une même mission : protéger les populations civiles libyennes, en opérant des frappes au sol contre des objectifs des forces pro-Kadhafi. Une opération totalement basée sur la projection de puissance depuis la mer.

Retour à bord… *« Poste de combat. Poste de combat ! »* Diffusé dans les coursives du bâtiment de projection et de commandement, ce message signifie qu'une mission du groupe aéromobile va débuter. Au cœur du bâtiment de guerre de 200 mètres de long pour 5 200 m² de pont d'envol, deux états-majors opèrent en simultané, celui des aéronefs et celui du navire. Dans le premier, dit « poste de commandement et de mise en œuvre » (PCMO), une douzaine d'hommes prend place à chaque fois qu'une mission est déclenchée. Les yeux rivés sur les écrans géants qui tapissent la pièce, chacun d'entre eux gère sa part des opérations : liaisons radio avec les aéronefs, veille de la situation tactique aérienne et navale, suivi de l'itinéraire de vol des hélicoptères… *« 21h29. Décollage du Puma dans quinze secondes »*, annonce l'officier « conduite » au commandant du groupement d'hélicoptères, le colonel M. *« Ce soir, le module s'articule autour sept machines. Deux appareils dédiés au sauvetage évoluent en retrait des hélicoptères de combat, ainsi que celui depuis lequel le chef des opérations commande les patrouilles. C'est avec lui que nous communiquons par radio pendant toute l'opération. »* La plupart du temps, les raids aériens, qui ont toujours lieu par nuit noire, suivent une chronologie identique : des objectifs sont déterminés en amont grâce aux divers capteurs de renseignements, mis en œuvre par l'Otan, dont la France (drones Harfang, pods de reconnaissance nouvelle génération emportés sur Rafale, Awaks, etc.) ; les hélicoptères reconnaissent ces objectifs ; enfin quand ils les ont formellement identifiés, ils les détruisent.

Jouxtant le PCMO, le « Central Opérations » (marine) coordonne l'environnement naval du théâtre. Pendant les phases de combat, dix opérateurs, qu'ils soient contrôleurs aériens, veilleurs radars ou officiers de quart, s'installent face à leurs consoles dans un épais silence. Avant la phase de décollage,

un écran retransmet les images prises par les caméras thermiques du pont d'envol. On y distingue les silhouettes des aéronefs et du personnel de pont qui gravite autour. En deux vagues, les patrouilles de Tigre et de Gazelle s'élèvent dans la nuit, feux éteints et liaisons radio en sommeil. *« Tant que les hélicoptères n'ont pas engagé le tir au-dessus du sol libyen, la discrétion est nécessaire à la fois pour la protection du bâtiment et pour l'effet de surprise qui accompagne leur arrivée sur zone »*, intervient le capitaine de frégate B., commandant des opérations (Comops). *Nous positionnons le BPC à bonne distance des côtes, à l'abri des éventuels tirs de batteries côtières,* précise le Comops. *Et nous surveillons toute menace qui apparaîtrait dans notre volume de détection, une attaque asymétrique par des embarcations chargées d'explosifs constituant le risque principal. Bien qu'affaiblies après plusieurs mois d'opérations, les forces pro-Kadhafi restent déterminées et peuvent plus que jamais agir de façon désespérée. »* Pour établir cette situation tactique, le Comops s'appuie sur les autres moyens engagés sur zone. Chaque raid d'hélicoptères s'intègre, *in fine*, dans une organisation de l'espace aérien globale et unique pour l'opération. Tous les aéronefs de « Unified Protector » doivent ainsi respecter scrupuleusement des itinéraires et des horaires prédéfinis afin d'éviter tout risque de colision et de tirs fratricides. *« Pendant les opérations aéromobiles, c'est depuis le CO du BPC que sont coordonnés les mouvements et les actions des deux frégates, du sous-marin et de l'avion de patrouille maritime qui sont engagés dans la force »,* précise le capitaine de frégate B. Recueil d'informations de différentes natures, surveillance aérienne et maritime ou encore tirs canon contre terre. ■■■

ARNAUD ROINÉ/ECPAD

Les hélicoptères de combat et de manœuvre de l'aviation légère de l'armée de terre sont embarqués sur le BPC. Leur mission intègre un volet important de coordination aéromaritime.

MARINE NATIONALE / EMA

Les mouvements et les actions des frégates, sous-marins et avions de patrouille maritime engagés sont coordonnées depuis le CO du BPC.

A chaque raid, le PC va vivre au rythme des comptes rendus radio et du balayage du radar sur lequel les points qui se déplacent symbolisent les aéronefs. Concentration maximale. Le calme qui prévaut ici contraste avec le fracas des tirs de roquettes et canon de 30 mm des Tigre et celui des départs de missiles Hot des Gazelle.

Une heure après les premières frappes, la phase d'exfiltration débute. *« Toutes les machines ont repassé la côte »,* annonce le commandant des opérations depuis son appareil. Pour le PCMO, la tension retombe doucement. Les contrôleurs aériens du CO, eux, se tiennent prêts à guider les aéronefs un par un pour l'appontage. Toujours plongé dans le noir, le bâtiment a été positionné face au vent pour faciliter leur approche. Reste à fournir aux pilotes les points GPS de l'axe qui va les mener « à l'aveugle » jusqu'à l'emplacement qui leur est réservé. *« Apponter en pleine nuit sur une plate-forme en déplacement, soumise au roulis et au tangage, est un exercice délicat pour les pilotes,* tient à souligner le colonel M. *Surtout après une mission intense qui a requis toute leur concentration. »* D'où la nécessité d'une coordination optimale avec le BPC, jusqu'au posé du dernier hélicoptère. *« L'engagement militaire de la France en Libye comprend un volet particulier de "projection de puissance de la mer vers la terre",* conclut le colonel M. *Seule une parfaite coordination des moyens et une imbrication étroite des actions du BPC et de l'Alat, dans un dispositif aérien complexe, permettent de mener cette opération sans précédent. »*

Cynthia Glock

ARMÉES D'AUJOURD'HUI

Quand la science

Face à la menace quotidienne que représentent les engins explosifs improvisés (IED), une structure européenne, actuellement dirigée par la France, vient de voir le jour. L'objectif du Labo C-IED : disséquer et analyser ces engins artisanaux. Reportage à Kaboul, en Afghanistan.

Dès avril 2010, une réunion de neuf ministres européens de la Défense a approuvé l'idée commune de création d'un laboratoire d'analyse criminologique afin de lutter contre les IED *(Improvised Explosive Devices)*. Doté d'un budget d'un million d'euros financé par l'agence européenne de défense (AED), le projet rassemble l'Autriche, l'Italie, le Luxembourg, les Pays-Bas, l'Espagne, la Suède, la Pologne, la Roumanie et la France. *« La France s'est portée volontaire pour être la nation cadre depuis l'initiative du projet en 2010 et pour encore 18 mois à compter du déploiement en Afghanistan. Elle voulait ainsi marquer sa volonté de voir le projet aboutir »,* insiste le chef de bataillon L., chef du labo contre-IED (C-IED), installé à Kaboul depuis septembre dernier. Après la désignation de la France comme nation-cadre, l'état-major des armées (EMA) a confié le dossier au général de division Ripoll, commandant l'Ecole du génie, qui occupe également la fonction otanienne de *Joint Chief Engineer* et dirige le pôle interarmées munitions et explosifs (PIAM). Le commandant L., alors affecté à la direction des études et de la prospective de l'Ecole du Génie, a été désigné début 2011 pour conduire ce projet. Il a fallu définir le profil du personnel à intégrer, assurer la formation et développer le laboratoire projetable lui-même. Le budget accordé par l'AED a été en grande partie utilisé pour cette phase de développement. Pour le déploiement, certains pays ont été directement mis à contribution : *« Le transport des 8 containers sur zone a été pris en charge par le Luxembourg quelques semaines avant le départ. La Suède a également fourni des équipements. Cet aspect multinational a été déterminant pour mener à bien l'aventure »,* affirme le commandant.

La recherche scientifique sur les IED n'est pas une démarche nouvelle en Afghanistan. Cette récente capacité européenne est le sixième laboratoire de ce type sur le théâtre, intégrée en complément d'un dispositif existant. A l'image d'un espace collaboratif, qui permet, lorsque plusieurs laboratoires constatent le même procédé dans l'élaboration d'un IED, d'en déduire qu'un individu ou un groupe détient cette capacité sur le territoire et tout faire pour le retrouver.

Petit retour sur le *modus operandi* antérieur : avant la naissance de ce labo, la chaîne IED fonctionnait sur deux échelons. Sur place, des équipes de niveau 1, appelées les *Weapon Intelligence Team* (WIT) avaient pour tâche principale de prélever des explosifs ou leurs déchets après explosions. On est ici dans la logique du gendarme qui récupère des éléments sur la scène de crime. Les différents éléments récupérés par les WIT (trace d'explosif, bidon ayant servi de conteneur, fil électrique, engrais, déclencheur…) étaient ensuite envoyés vers un laboratoire américain de niveau 2 à Bagram, voire un laboratoire en Europe ou aux Etats-Unis. Pour la France, il s'agissait de l'institut de recherche en criminologie de la gendarmerie nationale (niveau 3).

Implanté à Kaboul (Warehouse) depuis la mi-septembre 2011, le projet a pour objectif de mener, *in situ,* la chaîne complète des analyses scientifiques des différents composants d'engins explosifs artisanaux. Désormais, les éléments sont

L'intégration sur le théâtre

Le laboratoire C-IED intègre 14 personnes et 4 nationalités (hollandaise, espagnole, polonaise et française). Un conseiller de la DGA chef d'équipe Nedex (neutralisation, enlèvement, destruction des explosifs) apporte son expertise. Localisé sur le camp de Warehouse, il bénéficie du soutien français. Il agit sous commandement de l'ISAF Joint Command, qui intègre la Task Force Paladin. Cette TF est spécialisée dans la lutte contre-IED et travaille également au profit et en partenariat avec l'Afghanistan. Elle permet la mise en commun des données récupérées par les différents laboratoires.

fait parler les IED

JÉRÔME SALLES/ECPAD/EMA

Parmi les capacités du laboratoire figurent l'analyse de l'électronique et l'exploitation des données informatiques.

d'abord exploités au sein du labo contre IED (niveau 2) et ne quittent le territoire que pour des analyses très lourdes ne pouvant être effectuées sur Kaboul.

L'avantage d'un tel dispositif réside dans sa complétude et son action de proximité. Le fonctionnement de ce laboratoire repose sur un enchaînement méthodique des opérations.

Lorsqu'un IED arrive au labo, il faut d'abord s'assurer de son état inoffensif. C'est le travail des EOD (*Explosive Ordonance Disposal*), deux Français et un Hollandais, l'équipe de triage. *« S'il y a le moindre doute sur les éléments entrants, il est possible d'effectuer différentes analyses comme une radiographie dans une alvéole strictement sécurisée »*, précise un des membres de l'équipe. Suite aux vérifications, les éléments vont être empaquetés et une personne est chargée de suivre leur cheminement à travers les différentes cellules du labo.

Vient ensuite la séance photo avec l'adjudant S. : *« Chaque composant est photographié et archivé. Je suis parfois amené à travailler sur des petits objets : dans ce cas, il faut faire attention aux ombres portées qui peuvent masquer des détails. »*

Une fois passés sous l'œil du photographe, les éléments sont envoyés vers l'une des trois cellules spécialisées du laboratoire, selon le type de travail à effectuer. Une capacité du laboratoire concerne l'analyse de l'électronique et l'exploitation de données informatiques. Il s'agit de décortiquer les circuits intégrés, de chercher leur provenance, trouver les fréquences utilisées pour déclencher l'IED à distance. *« Je cherche à exploiter le maximum de données que l'on peut récupérer à partir d'un téléphone, disque dur, clé USB, GPS. Cela va des numéros de téléphone, aux photos et dans le meilleur des cas une localisation »,* déclare le maître G., en charge de la Media Exploitation.

La biométrie est également un axe majeur de la recherche, confiée conjointement à un Polonais, un Hollandais et un gendarme français. Empreintes et traces ADN permettent de déterminer la provenance et la traçabilité des engins *« Quand on reçoit les composants, on analyse leurs surfaces. Les procédés diffèrent selon leur porosité»*, explique l'adjudant M.

La dernière compétence du laboratoire concerne la chimie, plus précisément l'étude des produits utilisés pour la fabrication des explosifs. Le lieutenant D., chimiste, cherche à faire parler les produits : *« On retrouve souvent du nitrate d'ammonium, normalement utilisé comme engrais. Il faut être humble, le labo se met en place. Il ne va pas faire de miracles du jour au lendemain, mais il fait déjà la preuve de son efficacité. »*

Barthélemy Gruot

Concertation et dialogue social
Les rendez-vous électoraux de 2011

2011 est l'année électorale pour tous les agents civils de la fonction publique. Le 20 octobre, les civils de la défense ont élu leurs représentants au niveau national. Le second rendez-vous de cette année est fixé le 13 décembre prochain, au niveau local.

Les élections professionnelles de 2011 sont les premières à mettre en œuvre les accords de Bercy, qui modifient en profondeur le dialogue social dans la fonction publique, tant pour les administrations que pour les organisations syndicales. Au ministère de la Défense et des Anciens Combattants, ces élections sont d'une ampleur inédite, il s'agit d'organiser concomitamment quelque 250 scrutins différents pour près de 70 000 agents civils.

Désormais tous les agents civils du ministère, quel que soit leur statut, élisent directement leurs représentants au sein des comités techniques. Avec le renforcement de la logique d'élection, les organisations syndicales bénéficient d'une plus grande représentativité et d'une légitimité importante, éléments clés d'un dialogue social constructif et efficace. Le 20 octobre 2011, la communauté civile de la défense basée en métropole, en outre-mer et à l'étranger a voté pour le nouveau comité technique ministériel (CTM). 74 % des inscrits ont participé au vote.

Ce scrutin a permis, notamment, de déterminer la représentativité des partenaires sociaux au niveau national. Le 13 décembre 2011, les agents civils voteront plusieurs fois le même jour, pour la désignation de leurs représentants au niveau local, au sein des comités techniques de proximité, des comités techniques de réseau et des instances individuelles de concertation.

Ce qui change :

- harmonisation des cycles électoraux pour l'ensemble des trois fonctions publiques (de l'Etat, territoriale et hospitalière) ;
- élargissement des compétences des comités techniques ;
- abandon de la règle du paritarisme pour les comités techniques : désormais seuls les représentants du personnel prendront part aux votes ;
- il n'y a plus qu'un seul tour pour l'élection aux instances individuelles de concertation.

Pour plus d'informations sur Intradef : portail.sga.defense.gouv.fr, cliquez sur dossier Elections

JEAN-JACQUES CHATARD / DICOD

74 % des inscrits ont participé au scrutin du 20 octobre. Au niveau national, la répartition des 15 sièges de représentants est la suivante : FO : 4 ; UNSA-CGC : 4 ; CFDT : 3 ; CGT : 3 ; CFTC : 1.

ARMÉES D'AUJOURD'HUI

PAR BARTHÉLEMY GRUOT

11/11 LE CHEF DE L'ÉTAT PRÉSIDE LA CÉRÉMONIE DU 11 NOVEMBRE

Nicolas Sarkozy a présidé, à l'Arc de triomphe, la cérémonie nationale commémorative de l'armistice de 1918. La célébration a revêtu un caractère exceptionnel avec un hommage de la nation aux soldats morts pour la France. Un projet de loi va être déposé pour faire du 11 Novembre *« la date de commémoration de la Grande Guerre et de tous les morts pour la France »*. Pour la première fois, la Croix de la Valeur militaire a été décernée à titre collectif. Douze emblèmes qui se sont illustrés dans les opérations extérieures ont été décorés lors de la cérémonie.

P. SEGRETTE / PRÉSIDENCE DE LA RÉPUBLIQUE

07/10 LE PREMIER MINISTRE AU SÉMINAIRE D'OUVERTURE DES SESSIONS NATIONALES DE L'IHEDN ET DE L'INHESJ

Le Premier ministre, François Fillon, a prononcé vendredi 7 octobre un discours à l'occasion du séminaire des sessions nationales de l'Institut des hautes études de défense nationale (IHEDN) et de l'Institut national des hautes études de la sécurité et de la justice (INHESJ), qui avait lieu à l'École militaire, à Paris. Le Premier ministre a également évoqué les principaux sujets de politique extérieure, de défense et de sécurité sur l'année écoulée. Ce discours est en ligne sur : www.gouvernement.fr/gouvernement

ADC JEFF DE VOS / DEMS

JACQUES ROBERT

12/10 JEAN-PAUL BODIN, NOUVEAU SECRÉTAIRE GÉNÉRAL POUR L'ADMINISTRATION

Le contrôleur général des armées Jean-Paul Bodin a été nommé au poste de secrétaire général pour l'administration du ministère de la Défense et des Anciens Combattants, lors du Conseil des ministres du 12 octobre. Il a occupé le poste d'attaché d'administration centrale au ministère de l'Economie et des Finances à partir de janvier 1979 avant d'être admis à l'École d'administration des affaires maritimes. En 2007, il se voit confier les fonctions de directeur adjoint du cabinet civil et militaire du ministre de la Défense et des Anciens Combattants.

ECPAD

12/10 CHRISTIAN PIOTRE NOMMÉ AU POSTE DE CHEF DU CONTRÔLE GÉNÉRAL DES ARMÉES

Christian Piotre, 55 ans, prend la tête du contrôle général des armées. Ancien élève de L'École spéciale militaire de Saint-Cyr, il a notamment été chargé de mission puis conseiller pour les affaires administratives, sociales et du personnel au cabinet de François Léotard au ministère de la Défense de 1993 à 1995. Conseiller pour les affaires sociales, chargé du service national au cabinet du ministre de la Défense entre 1995 et 1997, il est ensuite nommé secrétaire général pour les affaires régionales auprès du préfet de la région Aquitaine à Bordeaux. Il occupait la fonction de secrétaire général pour l'administration.

10/10 UN MONUMENT NATIONAL POUR LES MORTS EN OPÉRATIONS EXTÉRIEURES (OPEX)

Le 10 octobre, à l'Hôtel de Brienne, le général Bernard Thorette, ancien chef d'état-major de l'armée de terre et président de l'association Terre Fraternité, a remis au ministre de la Défense et des Anciens Combattants, Gérard Longuet, en présence de Marc Laffineur, secrétaire d'État, le rapport relatif à l'édification d'un monument en hommage aux soldats morts pour la France en opérations extérieures. Ce mémorial devrait être érigé à Paris, dans un site prestigieux.

ROLAND PELLEGRINO/ECPAD

ARMÉE DE L'AIR

20/10 DES AVIATEURS FRANÇAIS À L'HONNEUR

Un mémorial en l'honneur d'aviateurs français ayant combattu au cours de la Seconde Guerre mondiale a été dévoilé lors d'une cérémonie religieuse organisée jeudi 20 octobre, en la cathédrale d'York (nord-est de l'Angleterre). Le général Jean-Paul Paloméros, chef d'état-major de l'armée de l'air (Cemaa), a assisté à ce vibrant hommage, en compagnie de son homologue britannique, l'Air Chief Marshal Sir Stephen Dalton. De nombreuses autorités étaient également présentes, dont le général Paul Fouilland, commandant les forces aériennes stratégiques.

17-21/10 L'« ARMADA DE L'ESPOIR » REPREND LA MER

Récompensée par le prix armées-jeunesse 2011 et forte du succès de sa première édition en 2010, l'*Armada de l'Espoir* a repris la mer du 17 au 21 octobre dernier. Au départ de Brest et à destination de Lorient, 130 jeunes ont participé à un parcours éducatif en mer. Cet embarquement visait à les sensibiliser aux enjeux citoyens d'aujourd'hui : le respect d'autrui, le mélange des cultures, le respect de l'environnement, le sens de l'effort et de la responsabilité… Il s'agissait également de permettre à ces jeunes de valoriser leurs mérites et de retrouver ou conforter leur confiance en eux.

JÉRÔME HARY/MARINE NATIONALE

ARMÉE DE L'AIR

20/10 PREMIÈRE PIERRE POUR LE CENTRE DE FORMATION NH90

La pose de la première pierre du Centre de formation interarmées du NH90 s'est déroulée au Cannet-des-Maures le 20 octobre. Le général de corps d'armée Jean-Philippe Margueron, major général de l'armée de terre, et le vice-amiral d'escadre Stéphane Verwaerde, major général de la marine nationale, ont coprésidé cette cérémonie sur la base Général Lejay. Le concept de ce centre est novateur : associer sur un même site la formation des équipages et des mécaniciens de l'armée de terre et de la marine nationale. La livraison des bâtiments est prévue en juillet 2012 pour accueillir 160 stagiaires en 2013.

CYBERES

le 5eme CH

DR

PACE
AMP DE BATAILLE

Communications, transports, énergie, santé, banques... l'informatique envahit aujourd'hui, et parfois à notre insu, notre quotidien. Les industries et les services essentiels à l'équilibre et à la prospérité des Etats reposent sur les systèmes d'information. La Défense n'y échappe pas. Des moyens radios aux messageries internes, des systèmes d'armes aux téléphones portables, le numérique est devenu l'incontournable outil de travail. Incontournable et vulnérable.

écoute, intrusion, destruction, prise en main de systèmes,

DR

Retrouvez ce dossier sur www.defense.gouv.fr
onglet cyberdéfense

la diversité des actions de piraterie informatique fait peser sur la communauté de défense une réelle menace. Une menace qu'il convient d'identifier au jour le jour, de contrer avec des solutions toujours nouvelles, de contrôler avec des moyens de sécurisation fiables et pérennes.

Après la terre, l'air, la mer et l'espace, le cyberespace constitue un 5e champ de bataille potentiel. Les nations se dotent de moyens pour en assurer la conquête et la défense. Les organisations internationales et les grandes puissances s'organisent. Objectif : créer une culture mondiale de la cybersécurité. En France, l'Agence nationale de la sécurité des systèmes d'information (Anssi) œuvre depuis 2009 à renforcer la cyberdéfense nationale. L'état-major des armées s'est par ailleurs récemment doté de structures dédiées.

Ce dossier établit un point de situation sur les menaces, les défis, les politiques et les dispositifs de lutte du cyberespace, dont chaque utilisateur est, consciemment ou non, un acteur de premier ordre.

Dossier réalisé par Nelly Moussu, Anne-Lise Llouquet et Grégoire Chaumeil.

Cyberespace // Monde

1

Cyberespace // France

2

1 Monde // Un enjeu in

Créer une culture mondiale de la cybersécurité

La coopération internationale est une des clés de la réduction des risques liés à la cybersécurité.

Dans un espace virtuel qui ne connaît pas de frontière, la coopération internationale revêt un intérêt capital. Elle se met en place progressivement. *« En matière de cyberdéfense, la coopération internationale est essentielle pour obtenir une vision claire et globale des menaces comme pour y répondre »*, estime Patrick Pailloux, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi). Ajoutant l'acte au discours, l'Agence a signé par exemple en novembre 2010 un accord de coopération avec le Centre Informatique estonien, mis en place par l'Otan, pour renforcer le partage d'information et d'expérience entre ces deux autorités nationales de cyberdéfense.

Collaborer est une nécessité pour se prémunir soi-même d'une attaque et riposter avec plus de force, car dans le cyberespace, les frontières géographiques ou étatiques n'existent pas. Les personnes, les objets, les systèmes informatiques y sont reliés. Un ordinateur situé en Allemagne peut infecter un système d'information français en envoyant un virus, qui aura transité par un système estonien (qu'il aura également infecté). La menace est donc transnationale.

En janvier 2011, le secrétaire américain de la Défense, William J. Lynn a rencontré des représentants de l'Otan et de l'Union européenne pour discuter de ces menaces. Au même moment, la Russie proposait à l'Otan de collaborer dans le domaine de la cyberdéfense. L'Organisation de coopération et de développement économiques (OCDE) mène également des travaux sur ce thème. En 2011, elle a publié un rapport sur la cybersécurité plutôt rassurant. *« Très peu d'événements [...] ont la capacité de provoquer un choc mondial »*, affirme le document. Néanmoins, il incite les Etats à se préparer à d'éventuelles attaques et encourage *« la ratification et l'utilisation généralisée de la Convention sur la cybercriminalité et d'autres traités internationaux potentiels »*. L'OCDE estime que *« la coopération internationale est une des clés de la réduction des risques de cybersécurité »*.

Coopération : les tentatives de l'ONU pour la cybersécurité

Dès 2002, les Etats-Unis et le Japon ont proposé une résolution sur la cybersécurité. La commission économique et financière de l'ONU l'a examinée. Elle traitait de la protection des réseaux électroniques mondiaux d'information et de l'Internet. Objectif : sensibiliser les acteurs pour créer une culture mondiale de la cybersécurité. Un programme onusien de cybersécurité a été lancé en 2007. En 2009, l'Assemblée générale de l'ONU s'est exprimée sur le sujet. Elle a invité *« les Etats membres à continuer de communiquer au Secrétaire général leurs vues et observations »*, notamment sur les problèmes en matière de sécurité de l'information, les efforts engagés au niveau national pour renforcer la sécurité de l'information et les activités de coopération internationale menées dans ce domaine.

Un an plus tard, une table ronde consacrée aux menaces et défis liés à la cybersécurité est organisée au sein de l'ONU. Gary Fowlie, chef du Bureau de l'Union Internationale des Télécommunications (UIT) à New York, a expliqué qu'il faudrait notamment prendre en compte les mesures juridiques et la coopération internationale

ternational

dans le cadre de la cybersécurité internationale. L'UIT a par ailleurs créé *« un groupe d'experts de haut niveau chargé de proposer une stratégie à long terme englobant les mesures légales, les mesures techniques visant à remédier aux failles des produits logiciels, ainsi que la prévention et la détection des attaques informatiques et la gestion de crise »*, note le sénateur Roger Romani en 2008 dans son rapport sur la cyberdéfense. Ce n'est qu'en mars 2010 que l'Assemblée générale de l'ONU a adopté une résolution pour la promotion d'une culture mondiale sur la cybersécurité. Son but : protéger les infrastructures de base. Le chemin vers une coopération est encore long. Des pays, comme la France, ont mis en place des *Computer Emergency Response Team* (CERT). Ces structures indépendantes informent les organismes qui s'y sont rattachés (administrations, centres de recherche, entreprises) sur les vulnérabilités et les moyens de s'en prémunir. Le *Forum of Incident Response and Security Teams* (FIRST), créé en 1990, favorise la coopération entre ces structures. L'*European Government Computer Security Incident Response Teams* (EGC) complète ce panel : il regroupe certains CERT gouvernementaux des pays européens.

Dans le cyberespace, les frontières géographiques et étatiques n'existent pas. Collaborer devient une nécessité pour se prémunir d'attaque et pour pouvoir répliquer avec force. Ici, au Centre Ops réseaux de l'US Air Force.

CÉCILIO RICARDO / US AIR FORCE

1 Monde // Otan

Enjeu du nouveau concept stratégique de l'Otan

Du fait de l'interconnexion des réseaux, les cyberattaques sont une menace internationale. Par leur coopération, notamment à travers l'Otan, les Etats peuvent renforcer leur cyberdéfense.

« Ce sont pas moins de 100 cyberattaques que l'Otan subit par jour », estime Jamie Shea, directeur de la planification politique de l'Alliance. Consciente de ces menaces et des conséquences potentielles pour ses activités, l'Otan a intégré la cyberdéfense dans son nouveau concept stratégique, adopté lors du Sommet de Lisbonne en 2010. Il place la cybersécurité *« au premier rang des nouveaux défis de sécurité que l'Otan et sa nouvelle division* Défis de sécurité émergents *devront relever dans les années à venir »*.

Dans un document, intitulé Engagement actif, défense moderne, les chefs d'Etat et de gouvernement se sont engagés à renforcer *« la capacité de l'Alliance à détecter et à évaluer les cyberattaques dirigées contre des systèmes revêtant pour elle une importance critique, à les prévenir, à s'en défendre et à s'en relever. Nous nous efforcerons en particulier d'accélérer l'évolution de la capacité Otan de réaction aux incidents informatiques (NCIRC) pour qu'elle atteigne sa capacité opérationnelle totale d'ici à 2012, ainsi que la mise en place d'une capacité centralisée de cyberprotection pour tous les organismes de l'Otan. »* Dès mars 2011, les ministres de la défense des pays de l'Otan ont approuvé un nouveau document en faveur du renforcement de la cyberdéfense otanienne. Pour l'instant, aucun calendrier décrivant les moyens et structures à mettre en place n'a été publié.

Un nouveau concept stratégique

Le concept stratégique de 2010 innove, car *« pour la première fois, un document de l'Alliance souligne que cette menace n'est plus le seul fait d'individus isolés ou de groupes criminels mais que des forces armées et des services de renseignements étrangers peuvent également être source d'attaques »*, remarque le Commandant Bertrand Boyer de la 18eme promotion de l'Ecole de Guerre, dans un article intitulé *La Cyberguerre, ou le mythe du blitzkrieg numérique.*

Une nécessaire coopération

Le concept de « cyberdéfense en profondeur », approuvé lors du sommet de Lisbonne, *« n'est pas destiné à être uniquement une stratégie militaire »*, a indiqué en février 2011 le général Abrial, commandant suprême allié Transformation de l'Otan, dans un article publié par le *New York Times*. D'autres acteurs clés doivent en effet être sensibilisés aux enjeux de la cyberdéfense pour assurer un niveau global de sécurité dans les systèmes d'information civils, dont les vulnérabilités pourraient impacter les militaires mais aussi toute la société. A la protection des systèmes d'information de l'alliance doivent s'ajouter ceux des Etats membres. Lors de la réunion cyberdéfense Otan du 25 janvier 2011, Francis Delon, secrétaire général de la défense et de la sécurité nationale (SGDSN) françaises, a appelé les nations à assurer *« la sécurité de [leurs] infrastructures de communications électroniques, et tout particulièrement de celles qui pourraient être utilisées par l'Alliance »*. Il a précisé que *« ces moyens, dont le choix doit rester à la discrétion de chacun, devront être interopérables, grâce à des standards et des procédures élaborés en commun »*. Pour promouvoir la coopération en matière de cyberdéfense, l'Otan a mis en place dès 2008 un centre d'excellence en Estonie. Des experts y élaborent notamment des stratégies militaires et des outils de lutte contre les attaques informatiques.

L'Otan devra partager ses informations afin de *« promouvoir le développement des capacités de cyberdéfense des Alliés »* et collaborer avec des entités comme l'ONU et l'Union européenne, pour développer notamment des concepts de cyberdéfense et des standards d'exploitation commune. *« Nous ne sommes pas les seuls à affronter l'émergence de nouveaux défis de sécurité, comme le terrorisme, la prolifération, le cyber, l'énergie ou la piraterie. Et personne ne peut les affronter seul efficacement. Nous devons donc développer un dialogue avec des pays comme la Chine, l'Inde et d'autres acteurs clés partout dans le monde »*, a recommandé le secrétaire général de l'Otan, Anders Fogh Rasmussen, lors d'une conférence de presse le 24 janvier 2011.

Genèse

Soucieuse de placer la protection de ses systèmes d'information au premier rang de ses préoccupations politiques, et de disposer ainsi d'une capacité de réaction, l'Otan a lancé un programme de coordination de la cyberdéfense lors du sommet de Prague en 2002. Il s'agissait alors de renforcer les capacités de l'Alliance à lutter contre les attaques informatiques. La politique de cyberdéfense de l'Otan a officiellement été entérinée en 2008 lors du sommet de Bucarest. Les chefs d'Etat et de gouvernement de l'alliance ont souligné *« la nécessité pour l'Otan et pour les pays de protéger les systèmes d'information clés conformément à leurs responsabilités respectives, de mettre en commun les meilleures pratiques, et de mettre en place une capacité visant à aider, sur demande, les pays de l'Alliance à contrer les cyberattaques. »*

BRUNO BIASUTTO/DICOD

L'Otan, dès 2002, avait déjà, dans un souci de protection de ses systèmes d'informations, lancé un programme de coordination de la défense lors du sommet de Prague.

Un cyberexercice made in Otan

L'Otan organise chaque année un exercice de cyberdéfense. En 2010, cette cybercoalition a réuni les organismes de l'Alliance et des représentants de 24 pays membres, dont l'Agence nationale de la sécurité des systèmes d'information pour la France. Son directeur général, Patrick Pailloux, souligne *« la richesse d'un tel exercice, qui met en rapport une diversité d'acteurs qui travaillent ensemble. Cybercoalition 2010 a été l'occasion pour l'Anssi de s'entraîner, avec ses homologues dans l'Otan et avec le ministère de la Défense, à gérer la dimension cybernétique dans les conflits. »* L'objectif était de mettre en place une coopération civilo-militaire et internationale pour faire face à des cyberattaques contre les moyens de transmission et les systèmes d'information des alliés.

Concept stratégique de l'Otan : www.nato.int

1 Monde // Union euro

Aux prémices d'une cyberdéfense commune

Avec l'inscription des enjeux cybernétiques dans ses textes officiels et la mise en place de structures et d'exercices dédiés, l'Union européenne se positionne dans le cyberespace.

En bonne place parmi les priorités de l'Union européenne, la sécurité informatique. Et pour cause : comme le rappelle le rapport de la Commission de défense sur la guerre informatique, paru en 2008 et présenté à l'assemblée européenne de sécurité et de défense, *« la raison d'être de la politique européenne de sécurité et de défense est d'élever le niveau de la défense européenne en développant des concepts, des techniques et des matériels européens. C'est une question d'autonomie politique et opérationnelle, et une affaire technologique et économique d'importance stratégique. »* Pourtant, l'Europe peine à mettre en place des moyens communs pour protéger ses systèmes d'informations et ceux de ses Etats membres.

En 2009, la Commission européenne a proposé une nouvelle stratégie. L'enjeu est d'abord financier : *« L'ensemble de l'économie européenne repose sur les services et réseaux de communications électroniques »*. Souhaitant préparer l'Europe à des cyberattaques de grande ampleur, elle a indiqué qu'il fallait faire un effort de sensibilisation *« pour permettre la mise en place de mesures de protection et de parades adéquates »*. Elle a également pointé *« le manque de coordination des approches nationales en matière de sécurité et de résilience (…), et une disparité de compétence et de préparation »*. Cette stratégie tient compte des remarques du rapport de 2008 (sur la mise en œuvre de la stratégie précédente) pour protéger les infrastructures critiques. Le document souhaitait des travaux supplémentaires *« afin d'envisager une approche globale de l'UE, de sensibiliser à ces questions et de renforcer la coopération internationale »*. La Commission européenne a donc proposé un plan d'action reposant sur la préparation (définir un niveau minimum de capacités entre Etats), la détection (développer un partage d'informations et d'alerte), la réaction (concevoir des plans nationaux en cas d'urgence) et la coopération internationale. Pour la première fois, un texte européen s'attaque à l'ensemble des problématiques cyber. Pour développer cette cyberdéfense, l'UE s'est dotée en 2004 de l'Enisa *(European Network for Information, Security Agency)*, l'agence européenne chargée de la sécurité des réseaux et de l'information. Ce centre d'expertise, chargé de surveiller les systèmes d'information et d'alerter les autorités en cas d'incident, conseille et assiste la Commission et les Etats membres de l'UE en matière de cyberdéfense. Il rédige notamment des rapports sur la cybersécurité des Etats membres. Mais son efficacité fait l'objet de débat à Bruxelles. En 2007, la Commission européenne a demandé l'évaluation de l'Enisa et a conclu que ses activités étaient *« insuffisantes pour atteindre le niveau élevé d'impact et de valeur ajoutée espérés »*. Le deuxième mandat de l'Enisa s'achève en 2011 et son avenir doit être réexaminé. Selon le rapport de la commission de défense sur la guerre informatique, transmis en 2008 à

> Une équipe d'intervention d'urgence sera capable d'intervenir dans tous les pays membres.

péenne

l'assemblée européenne de sécurité et de défense, c'est l'agence européenne de défense (AED) qui devrait mettre en œuvre une doctrine de la cyberguerre européenne. Les Etats membres de l'Union européenne ont d'ailleurs adopté un plan de développement des capacités européennes en 2008, élaboré par l'AED et prévoyant 12 actions prioritaires *« dont deux concernent directement la guerre et la défense informatiques »*.

« L'Union européenne est en mesure de se protéger contre une attaque informatique visant ses infrastructures vitales, mais il reste encore à assimiler à un crime la création et l'utilisation de logiciels malveillants », a annoncé la Commission européenne en 2010. Elle a présenté un projet de directive alourdissant les poursuites et les sanctions contre les hackers et les producteurs de logiciels connexes malveillants. Une collaboration policière et judiciaire renforcée entre les Etats est souhaitée.

En outre, l'UE a annoncé en juin 2011 qu'elle allait mettre en place une équipe d'intervention d'urgence capable de se déplacer dans tous les pays membres et de répondre aux cyberattaques visant ses institutions (Commission, Parlement, Comité des régions, etc.). C'est la première mesure active décidée par l'UE.

Mais la lenteur européenne dans le domaine de la cyberdéfense soulève un certain nombre d'interrogations. Le manque de motivation des Etats à collaborer à l'échelle européenne s'explique peut-être par l'existence d'accords bilatéraux : pourquoi développer en plus un accord européen ? Pour Michel Asencio, chercheur à la Fondation pour la recherche stratégique, la cyberdéfense commune n'est pas nécessaire car *« c'est une question de sécurité nationale »*. Daniel Ventre, ingénieur au CNRS, se demande quant à lui ce qu'il faut harmoniser. *« Le cadre juridique ? Mettre en réseau les cyber-unités de défense nationales ? La cyberdéfense imposerait de céder une part de ses propres prérogatives, de son pouvoir, de sa souveraineté, le partage d'instruments, d'accès, de réseaux, de moyens, etc. A quoi sont disposés les Etats ? »*

L'Europe organise des exercices de simulation

Cyber Europe 2010 a réuni les Etats membres de l'UE, l'Islande, la Norvège et la Suisse en novembre 2010 pour un premier exercice commun de cyberdéfense, en coordination avec l'Enisa. Cette opération s'inscrit dans le ca-dre d'une stratégie de renforcement de la sécurité informatique. L'objectif était *« d'évaluer l'état de préparation de l'Europe face aux menaces informatiques »*, a expliqué Neelie Kroes, commissaire européenne chargée des nouvelles technologies. D'autres exercices dans un cadre mondial seront mis en place pour continuer à améliorer la cybersécurité européenne.


UE 2009

Neelie Kroes, commissaire européenne chargée des nouvelles technologies, a annoncé que d'autres exercices de simulation seront mis en place pour préparer l'Europe à affronter les menaces informatiques.

ENISA : www.enisa.europa.eu

EXEMPLES DE CYBERATTAQUES

Les attaques informatiques, dont la première connue date de 1988, se propagent via Internet, une clé USB ou directement par un ordinateur pour empêcher, gêner ou détourner le fonctionnement des systèmes d'information ; autrement dit, elles visent à entraver l'utilisation d'un appareil informatique ou à voler des informations. Leurs cibles vont des particuliers aux grandes industries et aux gouvernements du monde entier. Depuis quelques années, les cyberattaques de grande ampleur se sont multipliées et ont démontré qu'aucune structure n'était à l'abri. Tour d'horizon de quelques attaques marquantes.

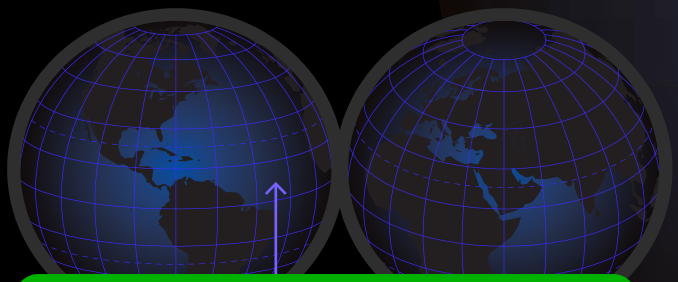
ETATS-UNIS

● ATTAQUE CONTRE UNE STRUCTURE DE COMMANDEMENT

En 2011, un virus informatique a infecté les postes de commande à distance des drones américains Predator et Reaper effectuant des missions en Afghanistan et sur d'autres théâtres. Le virus aurait été introduit dans les ordinateurs de la base via des disques durs externes.

● ATTAQUE CONTRE DES SITES GOUVERNEMENTAUX

En 2009, des cyberattaques ont visé des sites Internet américains. Parmi eux, les sites de médias, de la Maison Blanche, du département d'Etat, du ministère de la Sécurité intérieure, du ministère du Transport, de la *National Security Agency* (NSA), du Pentagone. Il s'agissait d'une attaque DoS (Déni de service) : les sites ne répondaient plus car ils étaient saturés par une multitude de demandes de connections simultanées.



MONDE

● ATTAQUE CONTRE DES SITES GOUVERNEMENTAUX

En 2007 des cyberattaques se sont produites en France, aux Etats-Unis, au Royaume-Uni, en Allemagne, en Nouvelle-Zélande, en Australie, au Canada, en Suisse, en Belgique, aux Pays-Bas. Elles visaient différents services des Etats (ministère des Affaires étrangères, diplomates, etc.), vraisemblablement à des fins d'espionnage. Un cheval de Troie (un programme informatique permettant de contrôler un ordinateur à distance) envoyé à diverses adresses mails a permis d'attaquer les sites de ces services.

● ATTAQUE CONTRE DES ENTREPRISES (Opération Aurora)

Cette cyberattaque, mise au jour en 2010, a visé plusieurs entreprises principalement américaines dont Google.

● ATTAQUE CONTRE DES ENTREPRISES / ATTAQUE CONTRE UNE STRUCTURE DE COMMANDEMENT (Virus Stuxnet)

En 2010, une attaque informatique via le virus Stuxnet a touché des infrastructures, notamment en Iran, en Inde, en Indonésie. Ce virus a infecté un logiciel Siemens destiné au Scada (*Supervisory Control And Data Acquisition*) qui contrôle les infrastructures industrielles vitales (eau, électricité, télécommunications, gaz, carburants, pipelines, raffineries, centrales nucléaires, etc.). Ce virus peut prendre le contrôle ou détruire le système Scada.

● ATTAQUE CONTRE DES SITES GOUVERNEMENTAUX (système Ghostnet)

En 2008, un système baptisé "Ghostnet" a été mis au jour par des chercheurs canadiens. Il permet, par l'infection de plusieurs ordinateurs, d'avoir accès à des informations confidentielles. Parmi les cibles : les bureaux du dalaï-lama (en Inde, à Bruxelles, à Londres, à New York), les ordinateurs d'ambassades (d'Allemagne, de Chypre, de Malte, du Portugal, de Roumanie, de Corée du Sud, d'Inde, d'Indonésie, de Malaisie, du Pakistan, de Thaïlande, de Taiwan, etc.), des ordinateurs des ministères des Affaires étrangères (d'Iran, du Bangladesh, du Bhoutan, de Lettonie, d'Indonésie, du Brunei, des Philippines, etc.), un ordinateur de l'Otan, des administrations françaises.

ROYAUME-UNI

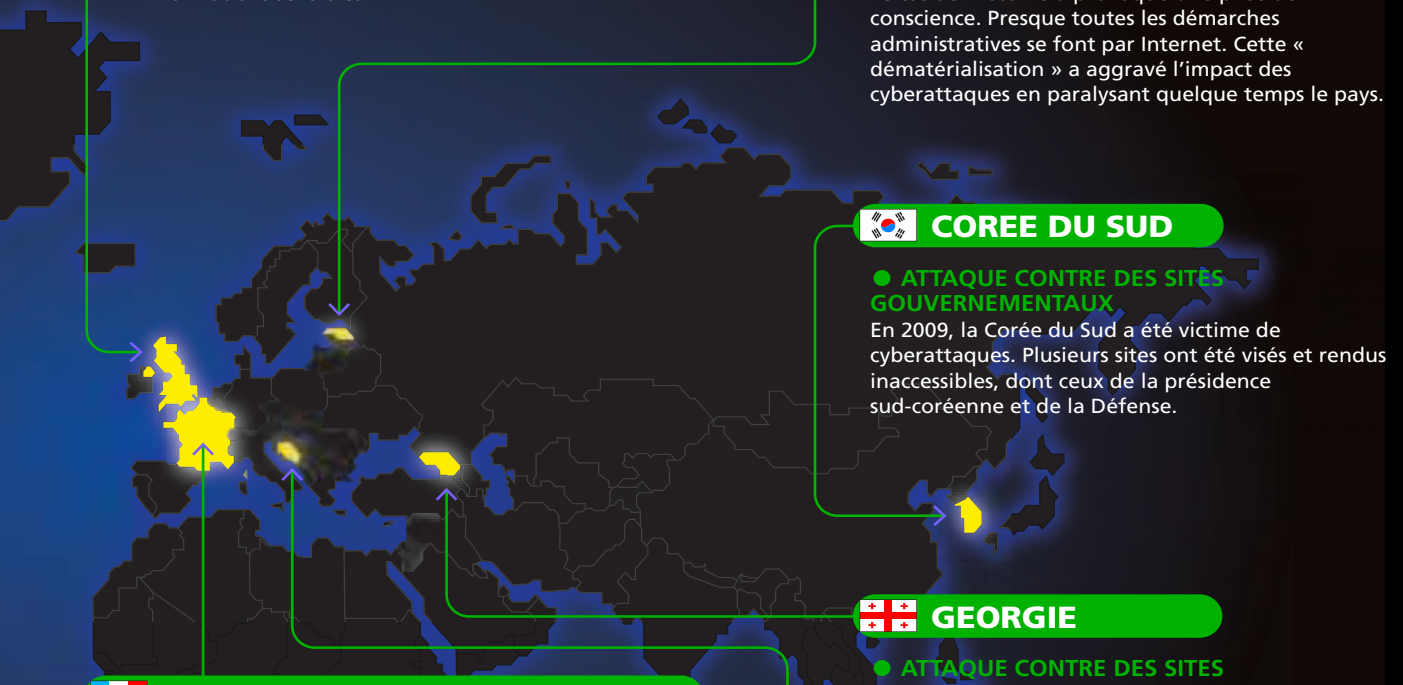
● **ATTAQUE CONTRE DES SITES GOUVERNEMENTAUX**

En 2010, le site Internet de la Royal Navy, la marine britannique, a été victime d'une attaque revendiquée par un groupe de hackers roumains, appelé TinKode. La technique utilisée par les pirates est appelée attaque par injection SQL : elle exploite la faille d'une application pour obtenir l'accès à des informations sensibles.

ESTONIE

● **ATTAQUE CONTRE DES SITES GOUVERNEMENTAUX**

En 2007, des attaques ont visé les sites du gouvernement, les banques, les médias estoniens et les opérateurs téléphoniques. Il s'agissait d'une attaque DoS (Déni de service) : les sites ne répondaient plus car ils étaient saturés par une multitude de demandes de connections simultanées. Le cas de l'Estonie a provoqué une prise de conscience. Presque toutes les démarches administratives se font par Internet. Cette « dématérialisation » a aggravé l'impact des cyberattaques en paralysant quelque temps le pays.



COREE DU SUD

● **ATTAQUE CONTRE DES SITES GOUVERNEMENTAUX**

En 2009, la Corée du Sud a été victime de cyberattaques. Plusieurs sites ont été visés et rendus inaccessibles, dont ceux de la présidence sud-coréenne et de la Défense.

GEORGIE

● **ATTAQUE CONTRE DES SITES GOUVERNEMENTAUX**

En 2008, des pirates russes et pro-russes ont « cyber-attaqué » la Géorgie lors des affrontements contre la Russie. Les sites du gouvernement, des médias et des infrastructures stratégiques (relais de communications, centrales électriques, approvisionnement en eau, banque nationale, etc.) ont été touchés par une attaque DoS (Déni de service) : les sites ne répondaient plus car ils étaient saturés par une multitude de demandes de connections simultanées.

FRANCE

● **ATTAQUE CONTRE DES SITES GOUVERNEMENTAUX**

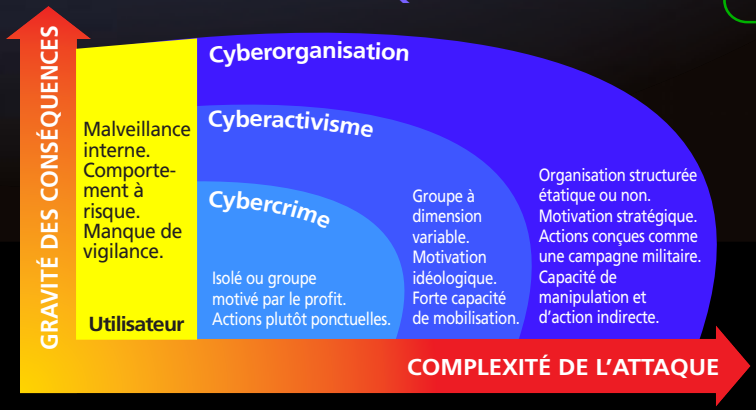
En 2006, une attaque a visé des centaines de sites français dont le ministère de l'Education nationale. Les hackers turcs protestaient contre le projet de loi sur la négation du génocide arménien. Les sites étaient « défigurés » : le drapeau turc et des messages apparaissaient.
En 2010, le compte Twitter du ministère des Affaires étrangères a été piraté. Un message d'insultes visant les Roumains et l'Union européenne avait été posté sur le compte.

OTAN

● **ATTAQUE CONTRE UNE STRUCTURE DE COMMANDEMENT**

En 1999, pendant la guerre du Kosovo, des hackers serbes ont attaqué les systèmes informatiques de l'Otan pour protester contre les bombardements alliés.

TYPOLOGIE DES ATTAQUANTS



2 France // Etat

2011 : la France affirme sa politique de cyber

En 2011, une stratégie en matière de lutte informatique défensive a été définie en même temps qu'une politique interministérielle. Objectifs : renforcer la cyberdéfense française.

« *En 2008, la France n'est ni bien préparée ni bien organisée.* » Tel est le constat du sénateur Romani, membre de la commission des Affaires étrangères, de la défense et des forces armées, et auteur d'un rapport intitulé *Cyberdéfense, un nouvel enjeu de sécurité nationale*. Depuis, le pays rattrape son retard. L'agence nationale de la sécurité des systèmes d'information (Anssi), créée en 2009 et rattachée au secrétaire général de la défense et de la sécurité nationale, assure à ce jour la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Préparant le pays à affronter les cyberattaques, elle a récemment publié une stratégie française de cyberdéfense.

Une stratégie publique…

En cas d'attaque majeure contre la nation, *« il y a nécessité d'une réaction immédiate et il ne faut pas de processus compliqué de concertation interministérielle »*, a souligné Francis Delon, le secrétaire général de la défense et de la sécurité nationale (SGDSN), lors d'une conférence en février 2011. L'Anssi homogénéise l'action des différents ministères, notamment à travers la stratégie de la France en matière de défense et de sécurité des systèmes, publiée en janvier 2011. La stratégie consiste essentiellement à développer une capacité de détection des cyberattaques et de créer un réseau de partenaires permettant un partage d'information nécessaire pour anticiper les vulnérabilités.

… et un plan d'action renforcé

En mai 2011, le Gouvernement a également décidé de renforcer son action pour la cybersécurité du pays. Cela implique notamment l'homogénéisation des capacités de protection des systèmes d'information de chaque ministère. Parmi les mesures prises, un *« groupe d'intervention rapide »* doit être créé pour *« traiter dans les meilleurs délais les attaques les plus graves »*, a annoncé le premier ministre François Fillon. Il permettra de soutenir les organismes publics et les opérateurs critiques (comme les sociétés de transport ou les hôpitaux), *« lorsque des indices laissent à penser qu'ils ont été l'objet d'une attaque informatique susceptible de présenter un danger pour la sécurité de leur activité, de menacer l'intégrité de leur patrimoine informationnel, de déséquilibrer le fonctionnement économique du pays ou de porter atteinte à la vie quotidienne des Français »*. Le renforcement de la cyberdéfense passera également par la croissance de l'Anssi. D'ici fin 2012, l'agence devrait atteindre un effectif de 290 personnes, et 360 en 2013.

La veille permanente

En cas d'attaques de grande ampleur, des mesures de sécurité des systèmes d'information ont été intégrées dans le plan Vigipirate. Il met en place une posture permanente de sécurité pour les systèmes d'informations, autrement dit une surveillance accrue des réseaux. Un plan de réaction aux cyberattaques a également été élaboré. Il s'agit du plan Piranet, auquel participent tous les acteurs concernés par la cybersécurité. En 2010, le SGDSN et l'Anssi ont organisé un exercice pour tester ce plan d'action et évaluer les répercussions d'une cyberattaque sur la société, les entreprises et l'Etat.

La prise de conscience du Livre blanc

« Dans les quinze ans à venir, la multiplication des tentatives d'attaques menées par des acteurs non

Anssi : www.ssi.gouv.fr

défense

étatiques, pirates informatiques, activistes ou organisations criminelles, est une certitude ». La France a clairement exprimé dans le livre blanc sur la défense et la sécurité nationale, publié en juin 2008, des mesures à prendre en matière de cyberdéfense. Par conséquent, *« la France devra développer une capacité de lutte »* dans le cyberespace. Pour une stratégie de défense et de sécurité adaptée aux menaces, le livre blanc a conduit à la création de l'Anssi pour *« renforcer la cohérence et la capacité propre des moyens de l'Etat »* en matière de prévention, de détection et de réaction aux attaques informatiques. Le livre blanc a également prévu la mise sur pied d'un centre chargé de la surveillance permanente des réseaux sensibles et de la mise en œuvre des mécanismes de défense adaptés. Il souhaitait enfin voir naître un réseau d'experts, avec une mission *« de soutien en formation et en conseil aux administrations locales »* et *« de remontée des signaux précurseurs d'incidents »*.

Le renforcement de la cyberdéfense passera également par la croissance de l'Anssi. D'ici fin 2012, l'agence devrait atteindre un effectif de 290 personnes et 360 en 2013.

3 QUESTIONS A PATRICK PAILLOUX, DIRECTEUR DE L'ANSSI

Quels sont les liens de l'Anssi avec le ministère de la Défense ?

Si l'ensemble des ministères dispose de capacités de protection de leurs réseaux informatiques, celui de la Défense en a plus que les autres, compte tenu de ses impératifs propres. Nous travaillons donc en collaboration avec l'ensemble des structures du ministère traitant de la cyberdéfense, notamment le Calid (voir p. 50) et la section Maîtrise de l'information de la DGA (voir p. 48).

Quels sont les objectifs de la stratégie de défense de l'Anssi ?

Il s'agit de faire de la France une puissance mondiale de la cyberdéfense. L'autonomie nationale doit être garantie en protégeant les informations les plus sensibles de l'Etat par des produits informatiques résistants aux cyberattaques. Il faut par ailleurs veiller à ce que nos infrastructures vitales, les hôpitaux, les centrales électriques et les transports, soient sécurisés. Enfin, la société de l'information doit être développée de manière harmonieuse et sûre.

Quelques mois après avoir défini ces objectifs, quels sont les ajustements ?

Le gouvernement a demandé à l'Anssi d'évaluer si les objectifs définis début 2011 étaient suffisants. De nouvelles mesures ont été élaborées. Le gouvernement a décidé de créer une équipe de projection en vue de renforcer la sécurité des systèmes d'information de l'Etat, en établissant par exemple des règles d'hygiène informatique pour tous les ministères (voir p. 47). Nous allons également nous assurer que l'ensemble des ingénieurs fraîchement diplômés, et notamment les informaticiens, connaissent ces règles de base. Enfin, nous allons bâtir un partenariat avec les opérateurs d'infrastructures vitales pour échanger et avoir un réseau d'alerte.

DR

Rapport du Sénat sur la cyberdéfense : www.senat.fr

2 France // Défense

Ministère : montée en puissance

En 2011, un concept interarmées a été élaboré et un officier général en charge de la cyberdéfense a été nommé.

Si l'Anssi agit au niveau interministériel, le ministère de la Défense et les forces armées conservent un rôle particulier dans ce domaine. Les militaires mènent des missions sous l'autorité du chef des armées, et leur cadre d'action ne se limite pas aux zones sous souveraineté nationale. Le ministère met donc en place des structures spécifiques pour protéger ses systèmes d'information, en collaboration avec l'Anssi.

Un officier général chargé de la cyberdéfense

Responsable de la cyberdéfense pour le ministère, le chef d'état-major des armées Edouard Guillaud estime que *« les systèmes d'information constituent aujourd'hui l'une des clefs de la supériorité opérationnelle des forces armées pour l'ensemble de leurs missions »*. Les protéger est donc devenu une priorité. Le contre-amiral Arnaud Coustillière en a la charge. Sous sa direction, le Calid, Centre d'analyse en lutte informatique défensive, surveille les réseaux et intervient sur des systèmes d'information infectés. Il travaille en collaboration avec le Centre opérationnel de la sécurité des systèmes d'information de l'Anssi. *« Il faut rapprocher les différentes structures dans un esprit de coopération, de mutualisation tout en respectant les responsabilités et les cadres d'actions respectifs »,* souligne le contre-amiral. Ces deux centres seront colocalisés à l'horizon 2014.

Protection et défense des systèmes

Au ministère, protection et défense des systèmes d'information sont traitées par des chaînes distinctes et complémentaires. La protection, animée par le fonctionnaire de sécurité des systèmes d'information, travaille sur du moyen terme et recouvre l'ensemble des moyens et méthodes établis pour protéger l'information, les systèmes informatiques et les réseaux de communication. Cinq autorités qualifiées mettent en place ces moyens techniques (cryptographie, mises à jour des antivirus, etc.) et organisationnels (formation, réseaux sécurisés, etc.). *« Ce sont des éléments actifs de sécurité »,* explique le commandant Mermod, chef du Calid.

La défense des systèmes d'information vise à garantir leur sécurité contre les cyberattaques en complétant les moyens de protection par des mesures réactives et une capacité de gestion de crise. Une posture permanente de détection des attaques, de réaction et de gestion de crise a été mise en place. Son objectif : rétablir le fonctionnement d'un système d'information le plus rapidement possible.

Jusqu'aux théâtres d'opérations

Ces mesures impliquent une planification, une analyse des effets de bords potentiels, une forte coordination des acteurs et une conduite rapide. L'impact opérationnel est également évalué, car couper un réseau peut mettre en péril une opération. Si le Calid détecte une anomalie sur un réseau militaire français déployé en Opex, il en rend compte au commandement du CPCO qui prend les mesures adaptées. L'objectif étant de préserver en permanence un lien sécurisé avec les théâtres d'opération.

Ces missions sont de plus en plus menées conjointement avec d'autres pays. L'état-major des armées participe aux travaux concernant la cyberdéfense avec les alliés. Il établit également des accords ou des procédures opérationnelles, et en informe l'Anssi. Par conséquent, le ministère de la défense a vocation à pleinement assumer la sécurisation de ses systèmes, en concertation avec l'Anssi.

EMA : une veille permanente

Officier général à la cyberdéfense à l'état-major des armées depuis le 1er juillet 2011, le contre-amiral Arnaud Coustillière assure une fonction nouvelle liée à l'ampleur prise par les aspects cybernétiques. Sous l'autorité directe du sous-chef « opérations » de l'EMA, il est en charge de la conduite de la lutte informatique défensive pour l'ensemble du ministère.

Dans quelle mesure le cyberespace est-il un nouveau champ d'action pour la Défense ?

Chacune des crises récentes a eu un volet cybernétique. A côté de la cybercriminalité qui se développe fortement, on voit aussi des attaques à visée stratégique à fin d'espionnage sur des secteurs de grandes industries, mais les évolutions techniques pour des effets plus perturbants sont aujourd'hui réunies. L'objectif du ministère de la Défense est de garantir l'efficacité opérationnelle des forces en opérations, et le bon fonctionnement courant du ministère. L'unicité et la rapidité de décision qu'offre une chaîne de commandement centralisée, spécialisée et pleinement adossée à celle de conduite et de préparation des opérations, est une condition nécessaire pour faire face au tempo des attaques informatiques.

Quelles sont les capacités de cyberdéfense au ministère de la Défense ?

Les opérateurs tels que la Dirisi, les armées, directions et services, établissent un premier niveau de sécurité dans leurs centres de supervision, où la majorité des menaces connues devraient pouvoir être traitées. En parallèle, l'échelon centralisé des capacités de lutte informatique défensive permettent de surveiller les anomalies des systèmes puis de déterminer la traçabilité d'une attaque, pour ensuite intervenir.

Au niveau opérationnel, la cellule cyberdéfense de l'EMA s'appuie sur le CPCO pour ce qui est de la conduite de crise ou du commandement des forces et sur le Calid pour tout ce qui concerne les capacités techniques (voir p. 50).

L'état-major des armées a rédigé un nouveau concept de cyberdéfense. Quel est son objectif ?

En juin 2010, l'ensemble des autorités du ministère a proposé au ministre que la défense informatique de nos systèmes soit confiée à une autorité unique, le chef d'état-major des armées (CEMA), afin de pouvoir réagir plus efficacement. Le concept de cyberdéfense signé par le CEMA le 12 juillet 2011, explique l'évolution du contexte et de la menace, les capacités dont il faut se doter pour s'en protéger, et les axes à développer pour y arriver. Il affirme que la cyberdéfense englobe toute l'informatique aussi bien dans les systèmes d'armes, les véhicules, les avions ou les navires. C'est un document opérationnel fondateur à partir duquel une doctrine sera proposée au CEMA à la fin de 2011.

Les 10 commandements cybernétiques

- **Tu passeras tes supports amovibles sur une station blanche et tu ne connecteras pas de supports personnels sur une station professionnelle.**
- **Tu effaceras toutes les données sensibles inutiles de tes clés USB avant de voyager.**
- **Tu rendras compte de toute détection virale aux organismes compétents.**
- **Tu vérifieras régulièrement qu'aucun équipement anormal n'est connecté sur ta station professionnelle.**
- **Tu utiliseras des mots de passe robustes.**
- **Tu ne laisseras pas ton mot de passe accessible.**
- **Tu ne communiqueras ton adresse mail professionnelle qu'à des personnes de confiance.**
- **Tu vérifieras l'expéditeur des mails que tu reçois.**
- **Tu seras vigilant avant d'ouvrir des pièces jointes à un courriel.**
- **Tu n'enverras pas de fichiers sensibles par Internet sans protection.**

MARINE NATIONALE

Intradef : ema.defense.gouv.fr

2 France // DGA

DGA Maîtrise de l'information : les artisans de la cy

Le centre DGA Maîtrise de l'information est l'expert technique de la Défense pour concevoir et évaluer des produits de sécurité.

La sécurité des systèmes gouvernementaux, qu'il s'agisse de systèmes d'information et de communication ou de systèmes d'arme, est, pour la DGA, une préoccupation de tous les instants. A Bruz, dans la région rennaise, le centre DGA Maîtrise de l'information abrite une grande part des meilleurs experts techniques gouvernementaux de la cyberdéfense. Un pool unique de compétences très variées et complémentaires capable de s'adapter aux évolutions de la menace informatique. *« Pour anticiper les attaques, il faut connaître et même anticiper les méthodes des attaquants… et veiller à ce que nos propres matériels et systèmes y résistent »,* explique Frédéric Valette, chef de la division sécurité des systèmes d'information (SSI). Dans un laboratoire, deux techniciens s'affairent autour d'un drone miniature non sécurisé, issu du monde civil. L'un deux, une télécommande à la main, fait décoller l'engin. L'autre, depuis son ordinateur, tente de prendre le contrôle de l'appareil. Quelques secondes lui suffisent pour s'accaparer des commandes du drone et se rendre maître de la maquette en vol : *« Lorsque la connexion n'est pas sécurisée, il me suffit d'écouter la transmission entre l'émetteur et le récepteur, d'interdire l'accès au pilote officiel et de continuer la séquence de commande ».*

« Pour anticiper les attaques, il faut connaître les méthodes des pirates. »

L'une des missions fondamentales de DGA Maîtrise de l'information en matière de cyberdéfense est d'acquérir une bonne connaissance actualisée de la menace. Mais elle en a d'autres : l'évaluation de la sécurité des systèmes d'information et, avant tout, la conception de produits de sécurité robustes. L'expertise de la DGA dans ces deux derniers domaines n'est pas nouvelle. *« La Défense s'est transformée au rythme des nouvelles technologies. Les réseaux ou les systèmes de réseaux de communication et d'échanges de données sont désormais au cœur de nos systèmes d'armes. Un missile, par exemple, recèle un nombre important d'informations transmises par télémesure, qui doivent aujourd'hui être protégées au même titre que des ordinateurs »,* assure Frédéric Valette. Charge aux techniciens et ingénieurs de la DGA de trouver les « cybersolutions » pour garantir la confidentialité et l'intégrité des informations et des systèmes support. *« La DGA est en charge de faire développer tout ce qui n'existe pas sur étagère dans le civil et de s'assurer que l'on répond bien aux besoins des forces* affirme Guillaume

BRUNO BIASUTTO/DICOD

bersolution

Poupard, responsable du pôle sécurité des systèmes d'information. *Nous sommes maître d'ouvrage et référent technique pour faire développer des produits de haut niveau de sécurité ».* Le chiffreur Echinops est l'un de ces produits.

Le chiffreur Echinops est un équipement qui permet de sécuriser les flux de réseaux les plus sensibles du ministère et de les protéger d'un attaquant contre les menaces d'écoute et de modification des données échangées. On les retrouve sur les navires de guerre par exemple. Le porte-avions *Charles de Gaulle* en possède une vingtaine pour assurer la sécurité de ses communications sensibles. Il suffit de placer cet équipement en émission et en réception d'une liaison pour que celle-ci soit entièrement protégée. Echinops a reçu l'agrément Secret Otan du Comité militaire de l'Otan et l'agrément Secret Défense délivré par l'agence nationale de la sécurité des systèmes d'information (Anssi). *« Nous avons suivi son développement depuis la conception des algorithmes et des composants cryptographiques jusqu'à l'évaluation finale de l'architecture sécurisée du système »*, rapporte Frédéric Valette. Les technologies de l'information évoluant rapidement, Echinops en est déjà à sa deuxième version.

Dernière innovation en date de la DGA, un téléphone cellulaire chiffrant, le Teorem, qui permet aux hautes autorités gouvernementales, aux états-majors militaires et aux cabinets ministériels français de téléphoner de manière totalement sécurisée. Ce mobile authentifie le correspondant grâce à un certificat numérique et affiche le niveau de sensibilité de la communication (secret défense, confidentiel défense). Actuellement, seuls deux États au monde sont ainsi équipés : les Etats-Unis et la France. Les premiers Teorem ont été livrés en septembre dernier. A terme, 14 000 exemplaires sont prévus dont la moitié d'entre eux seront destinés à la Défense. Le Teorem est un projet qui a mobilisé un nombre important d'ingénieurs pendant plusieurs années, essentiellement à DGA Maîtrise de l'information et chez le maître d'œuvre industriel. *« Le cahier des charges de nos produits de sécurité est la synthèse des spécifications fonctionnelles que nous recevons directement des forces et des spécifications techniques de sécurité interne à la DGA »,* explique Frédéric Valette avant de poursuivre : *« Nous établissons ainsi pour la DGA un plan d'actions des équipements à développer dans les 3 ou 5 ans à venir ».*

Aujourd'hui, DGA Maîtrise de l'information doit faire face à des systèmes d'informations ou des systèmes d'armes de plus en plus complexes qui empruntent un nombre croissant de technologies issues du civil. *« Les interconnexions de tous ces systèmes les rendent potentiellement plus vulnérables à des attaques informatiques,* rappelle Guillaume Poupard. *Plus il y a d'interconnexions plus il y a de possibilités de failles ou d'ouvertures non maîtrisées. Or, le partage et la sécurité sont deux notions souvent opposées. Nous faisons face à une extension des champs à protéger. Afin de conserver notre position de nation majeure sur la scène internationale, nous devrons demeurer capables d'interconnecter des systèmes de niveau de sécurité ou nationalité différents tout en garantissant leur cyberdéfense ».*

DR

Le Teorem, mobile ultra-sécurisé, destiné aux services interministériels. La moitié du parc équipera le ministère de la Défense.

En savoir plus : www.defense.gouv.fr/dga

2 France // De l'experti

Le Calid, l'expert du ministère

Veille, analyse, communication… Le Centre d'analyse de lutte informatique défensive assure une réaction rapide face aux menaces.

Toute la journée sur Internet, le sergent Julien P. effectue une veille des forums, blogs, réseaux sociaux, sites spécialisés et d'actualité qui abordent le thème de la sécurité informatique. Il recherche tout article évoquant les vulnérabilités et les techniques de cyberattaque diffusées sur la Toile. Il transmet certaines de ces informations aux analystes.

Ces derniers décryptent des programmes malveillants comme les virus ou les vers informatiques. Les analystes estiment leur impact et recherchent des solutions : soit ils trouvent des correctifs de sécurité existants, soit ils proposent des mesures de contournements en attendant l'élaboration d'un correctif par l'éditeur, soit ils développent un programme éradiquant le logiciel malveillant. Ces informations sont transmises à un coordinateur qui alerte les autorités concernées, transmet les solutions aux unités touchées et réalise des comptes-rendus pour l'officier général chargé de la cyberdéfense auprès du chef d'état-major des armées.

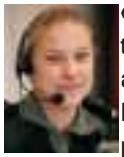
Le Calid participe en permanence à la protection des systèmes d'information, en collaboration avec les autres entités ministérielles en charge de la sécurité informatique. *« Pour l'instant, on ne constate pas de vols de données ou de mise en péril des systèmes d'armes sur les théâtres à travers les systèmes d'information »,* rassure le commandant Mermod. Mais la menace existe. *« Lors de la conduite de tirs, un commandant décide des opérations en fonction des informations qui apparaissent sur ses ordinateurs : c'est un risque de vulnérabilité car ces informations peuvent être piratées ».* La mise en place de sondes de détection sur tous les réseaux du ministère fait l'objet d'un programme d'armement. Ces sondes ont pour mission de remonter automatiquement toutes les informations du niveau local vers le centre d'analyse, *« pour être aux prémices de l'attaque ».*

TEMOIGNAGES

Michael M., technicien coordinateur

« J'ai un rôle de communicant : je récupère auprès de différentes entités des informations, j'en alerte d'autres. Il y a quelques mois, un CERT (computer emergency response team) m'a prévenu que des données personnelles de militaires (leurs comptes Internet, login et mot de passe, numéro de carte bancaire…) avaient été volées. J'ai alors prévenu les personnes concernées et je leur ai proposé des solutions pour que ça ne se reproduise pas, comme un mot de passe plus élaboré. »

Adjudant Sabrina D., analyste



« Mon métier consiste à tester des correctifs, autrement dit à corriger les failles informatiques pour, par exemple, contrecarrer un virus. Un virus est un code malveillant : à moi de le décrypter pour connaître les problèmes qu'il peut engendrer. »

Sergent Julien P., veilleur

« Je fais de la veille Internet. Parmi mes sources d'information, il y a Twitter et les blogs. Lorsque je trouve l'existence d'une faille informatique dans un logiciel ou de nouveaux moyens d'attaques disponibles sur la Toile et qui pourraient impacter le Mindef, je recoupe mes informations pour vérification. Je les publie ensuite sur l'intradef afin d'informer le personnel et les administrateurs du Mindef. »

PHOTOS : C.FIARD/DICOD

se au terrain

Au niveau tactique

La conduite des opérations inclut une composante cyberdéfense. Chaque unité (GTIA et détachement air) rend compte au Comsic (commandant des systèmes d'information et de communication) de théâtre, conseiller du commandant de la force.

Dès le déploiement des unités sur le théâtre, le Comsic met en place un réseau opérationnel sécurisé (anti-virus, moyen de chiffrement, firewalls…) sur l'ensemble de la force. Assisté de l'OSSI de théâtre, il est chargé de mettre en place l'organisation humaine et matérielle nécessaire, de maintenir le niveau de sécurité, de contrôler le respect des règles de sécurité et de superviser les réseaux opérationnels.

Autre conseiller du domaine pour le Comanfor, un officier LID (lutte informatique défensive) est désigné. Non spécialiste de la cyberdéfense, son rôle est de déterminer et de présenter au commandant de la force les impacts d'une attaque sur ses capacités opérationnelles : en termes d'effets, il fait le point des dommages, des systèmes d'armes rendus inutilisables ou dont la fiabilité pourrait être remise en cause.

Le Comsic est subordonné, dans la chaîne opérationnelle, au CPCO (centre de planification et de conduite des opérations). En cas de cyberattaques majeures sur un théâtre, une cellule de crise est mise sur pied au CPCO et dirigée par l'officier général cyberdéfense.

Parallèlement, les techniciens du Comsic sont en liaison directe avec le centre d'analyse en lutte informatique défensive dont les directives vont permettre de limiter les effets de l'attaque et si nécessaire neutraliser les logiciels malveillants (virus, vers, cheval de Troie) qui auraient pu s'introduire dans les réseaux.

SIRPA TERRE

En cas de cyberattaques majeures sur un théâtre, une cellule de crise est mise sur pied au CPCO et dirigée par l'officier général cyberdéfense.

Intradef : www.calid.defense.gouv.fr

Glossaire

La cyberterminologie pour les nuls

Cyberespace, cyberdéfense, cyberguerre… Petit décryptage en attendant leur entrée dans Le Robert.

L'objet : la cyberdéfense

« Ensemble des mesures techniques et non techniques permettant à un Etat de défendre dans le cyberespace les systèmes d'information jugés essentiels. » (source Anssi). Ces mesures peuvent être défensives (surveiller un ordinateur, le protéger avec un anti-virus, réparer les dommages causés par ce virus) ou offensives (créer un virus pour attaquer l'envahisseur).

Le lieu : le cyberespace

C'est un espace de communication virtuel, composé d'appareils interconnectés bien réels : ordinateurs, smartphones, GPS, etc. Ces objets sont reliés à travers un réseau informatique allant de l'intranet d'une entreprise à Internet. Cet espace ne connaît pas de frontières géographiques : les échanges informatiques se font d'un Etat à un autre. Il n'y a pas non plus de frontières physiques : ce qui survient dans le cyberespace peut impacter le monde réel (en infectant un ordinateur, on peut contrôler un objet qui lui est connecté).

La menace : les cyberattaques

C'est un acte malveillant de piratage informatique dans le cyberespace. Les cyberattaques peuvent être l'action d'une personne isolée, d'un groupe, d'un Etat. Elles incluent la désinformation, l'espionnage électronique qui pourrait affaiblir l'avantage compétitif d'une nation, la modification clandestine de données sensibles sur un champ de bataille ou la perturbation des infrastructures critiques d'un pays (eau, électricité, gaz, communication, réseaux commerciaux). Ces actes peuvent être motivés par l'appât du gain ou par intérêts politiques ». La cyberdéfense du ministère de la Défense français vise à détecter et contrer les cyberattaques dont la cible et la finalité sont liées au ministère et à la Défense.

Formes de cyberattaques

- La cybercriminalité est un acte contrevenant aux traités internationaux ou aux lois nationales effectué dans le cyberespace ou au moyen d'un système informatique.
- Le cyberespionnage est un piratage informatique qui permet d'accéder à des informations tenues secrètes. L'objectif est d'en tirer un avantage personnel, économique, politique ou militaire.
- Le cyberterrorisme est un « acte de terrorisme utilisant des systèmes informatiques ou la technologie des ordinateurs comme une arme ou comme une cible (…). Le cyberterrorisme a des motivations politiques, sociales ou religieuses, il vise à semer la peur ou la panique dans la population civile ou à déstabiliser l'appareil militaire et civil. » (Otan)
- La cyberguerre est un conflit « classique dont au moins une des composantes, dans la réalisation, les motivations et les outils (armes au sens large du terme) s'appuie sur le champ informatique ou numérique. Ces composantes sont dénommées cyberattaques » (Source : Eric Filiol, auteur et expert en sécurité informatique et ancien militaire). Son objectif est politique : elle cible les militaires, un Etat (et ses infrastructures) ou une société. Il ne faut pas confondre avec la guerre de l'information (altération de l'image de son adversaire via les médias et les outils du cyberespace) et la guerre électronique (contrôler ou détourner les émissions radioélectriques) d'un adversaire.

Pour être au cœur de la défense

Chaque mois, découvrez nos *forces en action*, les enjeux de notre stratégie de défense, les facettes de l'industrie et des technologies de l'armement. Participez aux débats des armées et renforcez votre culture militaire. Avec ses 68 pages et sa version online, *Armées d'aujourd'hui* est le magazine indispensable de ceux qui veulent des repères pour la défense d'aujourd'hui.

Abonnement	Public			Personnel de la défense*		
	France	Dom-Tom par avion	International par avion	France	Dom-Tom par avion	International par avion
1 an (10 n°)	20 €	30 €	35 €	15 €	25 €	30 €
2 ans (20 n°)	35 €	55 €	65 €	25 €	45 €	55 €

*** Personnel de la défense, réserviste, étudiant, lycéen, correspondant défense (sur justificatif).**

Abonnez-vous !

BULLETIN D'ABONNEMENT

Nom et prénom ..... Grade ou fonction .....

Adresse ..... Localité ..... Code postal .....

Renseignements statistiques

Âge ..... Profession ..... Secteur d'activité ..... Nom de l'entreprise .....

Abonnement souhaité

☐ Normal ☐ Spécial* ☐ France ☐ Étranger/Dom-Tom/Par avion

☐ 1 an ☐ 2 ans Nombre d'exemplaires ☐

*** Personnel de la défense, réserviste, étudiant, lycéen, correspondant défense (sur justificatif).**

ARMÉES D'AUJOURD'HUI

Joindre à la commande le règlement à l'ordre de : M. l'agent comptable de l'ECPAD, et envoyer celui-ci à :
ECPAD / Service abonnements, 2 à 8 route du Fort / 94205 Ivry sur Seine CEDEX. Tél. : 01 49 60 52 44 - Fax : 01 49 60 59 92. Email : routage-abonnement@ecpad.fr

Les informations recueillies dans ce document sont nécessaires au traitement de votre commande et destinées à nos services internes. Elles ne sont en aucun cas communiquées et peuvent donner lieu au droit d'accès et de rectification prévu par l'article 27 de la loi du 6/01/1978.

Rencontres territoriales

Le cycle des rencontres territoriales entre le ministre de la Défense et des anciens combattants et les acteurs de terrain de la réforme est en cours et se poursuivra jusqu'au mois de décembre. Retour sur Lille et Toulon où se sont tenues les deux premières.

A mi-parcours de la réforme et dans une période de forte activité opérationnelle, Gérard Longuet s'est rendu à Lille et à Toulon, respectivement les 7 et 21 octobre, pour recueillir les témoignages et questionnements des cadres en région. *« En tant que personnel impliqué dans la réforme, vous avez le devoir de nous faire remonter les problématiques que vous rencontrez chaque jour et c'est à nous de pouvoir rectifier telle ou telle mesure »*, a-t-il annoncé lors de la première rencontre à Lille, le 7 octobre. *« Vous êtes les architectes de la réforme »*, a tenu à préciser le ministre aux personnels de la zone de défense Sud. *« Les réunions que nous tenons cet automne ont un objet précis : réfléchir à l'amélioration d'une réforme opérationnelle qui repose aux trois quarts sur la fonction soutien. »*

ROLAND PELLEGRINO / ECPAD

Ces sept séminaires vont permettre un véritable échange entre Gérard Longuet et le personnel impliqué dans les réformes.

A Lille, comme à Toulon, les échanges avec le personnel ont mis en avant certaines difficultés administratives. C'est le cas notamment sur la base aérienne 103 de Cambrai où la flotte aérienne se voit sous la menace potentielle d'une interruption d'approvisionnement de produits indispensables pour assurer ses missions, tels l'oxygène et l'azote liquide qui font l'objet d'un marché national. *« La transformation de nos armées a profondément chamboulé notre paysage administratif avec l'émergence de nouvelles structures, l'évolution de périmètres de responsabilité »*, a expliqué au ministre le chef soutien du personnel et chef d'antenne du GSBdD de Lille. Les conséquences tirées par la BA 103 montrent que le nombre d'interlocuteurs a été multiplié en 2011, ce qui engendre des factures parfois erronées, ou non payées au fournisseur. Interrogé sur la complexité de certaines démarches administratives, le général Eric Rouzaud, commandant interarmées du soutien, a rappelé lors de ces deux rencontres que tous les processus n'étaient pas encore arrivés à maturité. *« Il faut que l'on travaille sur la comptabilité des matériels et sur la prise en compte des risques. »* Ceci étant, il ressort des deux rencontres que lorsque les outils informatiques sont déployés, les démarches s'en trouvent simplifiées. *« Lorsque j'étais chef de corps, il fallait que je m'organise pour trouver des lits, de la nourriture, des voitures quand nous partions en exercice ou en mission. Aujourd'hui, on s'adresse à un unique interlocuteur qui doit trouver les solutions »*, a expliqué le commandant de la base de défense de Marseille, base dans laquelle a été déployé le logiciel Sillage permettant de dématérialiser les procédures administratives liées au soutien commun.

A Toulon, les réflexions portant sur les opérations ont été nombreuses. Les unités de cette zone sont en effet particulièrement engagées dans les activités opérationnelles liées à Harmattan. La BdD de Toulon est concernée par les appareillages et par les flux logistiques denses des bâtiments de la flotte. Les BdD d'Istres et de Solenzara mènent quant à elles des missions opérationnelles au quotidien qu'il faut pouvoir soutenir. En janvier prochain, après les sept rencontres organisées en région avec le personnel militaire et civil, une synthèse sera effectuée et devra permettre de simplifier et d'améliorer certaines procédures. *« Vous êtes au milieu du gué. La réforme doit continuer et aller à son terme, nous ne pouvons pas nous permettre de faire de pause à mi-parcours »*, est aussi venu rappeler le ministre.

Paul Hessenbruch

« La réforme doit continuer et aller à son terme... »

Calendrier des rencontres territoriales sur la réforme

- **Saint-Germain-en-Laye : 8 novembre**
- **Rennes : 17 novembre**
- **Bordeaux : 24 novembre**
- **Lyon : 1er décembre**
- **Metz : 8 décembre**

Interview d'Olivier Vasserot, nouveau délégué aux restructurations

« Les acteurs locaux sont au rendez-vous des restructurations de défense. »

La délégation aux restructurations (DAR) est chargée de la préparation, du suivi et de l'accompagnement des restructurations de défense. Sa mission : mettre en place un dispositif d'accompagnement qui puisse *« recréer un volume d'emploi et d'activité comparable à celui supprimé par les restructurations. »*

Quels sont les moyens dont dispose la DAR pour parvenir à ses objectifs ?

L'Etat a naturellement intégré le traumatisme économique et le choc moral que pouvaient représenter les fermetures de ces sites, aussi une enveloppe de 320 millions d'euros a-t-elle été allouée dès 2008 pour mettre en place des mesures concrètes d'ici 2015. Nous avons identifié 58 sites les plus touchés par les restructurations. Des contrats de redynamisation signés entre l'Etat et les territoires touchés doivent permettre de compenser le départ de la défense. Ces contrats prennent la forme de CRSD ou PLR en fonction de l'ampleur des restructurations*. Aujourd'hui, 23 contrats de sites ont déjà été signés, 25 autres devraient l'être d'ici la fin de l'année et dix autres en 2012.

DR

Olivier Vasserot, contrôleur général économique et financier nommé délégué aux restructurations (DAR) le 1er septembre 2011.

Justement, comment sont préparés ces contrats et qui les établit ?

Nous suivons cette réforme depuis le début pour donner de la cohérence avec la loi de programmation militaire. Pour les 58 sites touchés, la DAR a missionné des cabinets d'audit pour détailler les forces et les faiblesses économiques des territoires. Nous nous appuyons aussi sur nos dix délégués régionaux aux restructurations qui travaillent avec les services préfectoraux. Une fois l'expertise réalisée, la DAR, en collaboration avec les acteurs locaux, dresse un plan d'actions visant à redynamiser les territoires touchés par les restructurations. Les mesures issues de ces plans font appel aux subventions étatiques prévues dans l'enveloppe globale de 320 millions d'euros.

Sur quels critères décidez-vous d'attribuer des subventions ?

L'objectif d'une mesure est de récréer des emplois. Mais il faut aussi qu'elle soit en cohérence avec les richesses, les particularités et les besoins du territoire touché : sur une emprise militaire mise à disposition, telle commune développera un centre scolaire, telle autre un centre d'hébergement pour « seniors ». La DAR organise en quelque sorte l'antithèse d'une délocalisation « brute de décoffrage », comme on en voit malheureusement trop souvent dans le secteur privé. Il fallait aller au-delà de la compensation financière, même si elle est non négligeable, car un des écueils de ces redynamisations aurait été de distribuer ces subventions sans se soucier de leur utilisation.

Sur les 23 contrats de site déjà signés, quel bilan pouvez-vous faire ?

A ce jour, l'Etat a investi près de 137 millions d'euros pour redynamiser les territoires, sur une dotation initiale de 320 millions d'euros. Celà étant, le montant global des contrats signés représente une valeur de 770 millions d'euros. Chaque euro dépensé par l'Etat a donc permis, par un effet de levier, une contribution des collectivités cinq fois supérieure. En soi, c'est déjà un grand motif de satisfaction de voir que les acteurs locaux s'impliquent dans la transformation de leurs territoires. C'est bien la preuve d'une adhésion unanime et indispensable à la politique de redynamisation.

Je répète volontiers aux élus que je rencontre depuis ma nomination, à quel point cette réforme est pour eux l'opportunité de développer de nouvelles activités. En construisant une économie moderne, ils garantissent leur autonomie et leur devenir.

Concrètement, en termes de création d'emplois, quels sont les premiers résultats ?

On enregistre d'ores et déjà des résultats, même si l'ensemble des projets n'en sont qu'à leurs prémices. Il faut du temps pour les mettre en œuvre et constater un retour sur investissement. A l'exemple d'un des premiers contrats de redynamisation, signé en mai 2009 à Barcelonnette, on sait aujourd'hui que six entreprises se sont installées en 2010 et 37 emplois ont été créés. D'autres projets commencent à prendre forme, comme la création d'un hôtel d'entreprise, d'un centre de balnéothérapie et d'une maison franco-italienne. Une antenne de l'université de Grenoble a même vu le jour pour accueillir étudiants et chercheurs dans les domaines de la biodiversité (projet Soleane). Tous ces projets prennent bien en compte la spécificité de la région, ce qui ne peut que favoriser leur pérennité. Enfin, dès la fin des signatures de contrats prévue pour la fin du premier semestre de 2012, nous devrons assurer le suivi de la mise en œuvre de l'ensemble des actions programmées, en veillant à ce que les résultats escomptés soient effectifs. ■

Pour plus d'information, consultez : www.restructurations.defense.gouv.fr

Propos recueillis par Paul Hessenbruch

** Le contrat de redynamisation de site de défense (CRSD) s'applique à un périmètre réduit autour du site libéré. Les plans locaux de redynamisation (PLR) s'adressent, eux, à l'ensemble d'un département.*

BRÈVES MODERNISATION

IMPLANTATION

Le 503e Régiment du train arrive à Nîmes

430 véhicules militaires, 150 containers et tout l'armement du 503e Régiment du train ont été transférés sur la base de Nîmes-Garons. La cérémonie d'installation s'est tenue le 16 septembre 2011. Le régiment et ses familles forment une communauté d'environ 2 000 personnes. 200 militaires

S. CERDAN/503e RT

supplémentaires arriveront à l'été 2012, avec l'intégration d'un escadron de transport de blindés, d'un peloton de circulation routière et de l'équipe enduro motocycliste de l'armée de terre.

FLOTTE AÉRIENNE

La DGA livre le dernier Awacs français rénové

La direction générale de l'armement (DGA) a livré le 7 octobre 2011 le 4e avion-radar SDCA avec système de communications rénové (SDCA : système de détection et de commandement aéroporté — Awacs en terminologie Otan).

La flotte des Awacs français comprend 4 appareils en service dans l'armée de l'air depuis le début des années 90. Véritables « sentinelles volantes », ces avions ont pour mission la détection et la surveillance ainsi que le contrôle et la conduite des opérations aériennes militaires.

La DGA a notifié en 2008 pour 50 M€ un marché de rénovation de ces avions à la société Air France Industries. Outre le maintien en conformité avec l'évolution des réglementations édictées par l'organisation de l'aviation civile internationale (OACI), cette rénovation vise à garantir le maintien de leur interopérabilité et de leur interchangeabilité avec les Awacs de la Royal Air Force, de l'Otan et de l'US Air Force.

CYRIL AMBOISE/SIRPA AIR

TERRITOIRE

Signature du plan local de redynamisation de Meurthe-et-Moselle

Gérard Longuet, ministre de la Défense et des anciens combattants, a assisté à la signature du plan local de redynamisation (PLR) de Meurthe-et-Moselle. Ce document a été signé jeudi 13 octobre entre l'Etat et les acteurs locaux pour faire face aux changements provoqués par les réorganisations des sites de défense.

Ce PLR est le résultat d'une volonté d'accompagnement économique territorial faisant suite à la fermeture d'unités, en particulier celles de l'état-major de la 4e brigade aéromobile à Essey-lès-Nancy, dont les fonctions sont désormais mises en œuvre par le commandement des forces terrestres de Lille (CFT).

Le plan d'un montant de 3 M€ se décline en 3 axes stratégiques de développement économique : le premier vise à favoriser la création d'emplois. Le deuxième consiste à encourager l'implantation de nouvelles entreprises. Le troisième axe doit permettre le développement de celles qui sont déjà implantées (zones d'activité, pépinière d'entrepri-

R. PELLRGRINO/ECPAD

SANTÉ

Le service de santé des armées choisit d'adhérer au RESAH-IDF

Dans le cadre de sa politique d'amélioration de la performance des achats, le Service de santé des armées (SSA) a décidé d'adhérer au Réseau des acheteurs hospitaliers d'Ile-de-France (RESAH-IDF). Cette adhésion s'inscrit dans une politique d'achat fondée sur la performance économique qui prend en compte les autres acteurs en matière d'achat du système de santé (UGAP, syndicats interhospitaliers, Uniha…).

Cette centrale d'achat, dont le volume d'achat est de l'ordre du milliard d'euros, regroupe une grande partie des établissements de santé franciliens et est un des principaux acteurs de la réforme des achats menée par le ministère de la Santé.

Outre l'accès aux marchés du Resah dans le cadre des stratégies d'achat du SSA, la participation à ce réseau permettra de mener des actions de benchmarking et d'échanges de bonnes pratiques entre grands acheteurs du système de santé.

Si les premiers bénéficiaires de cette adhésion seront les établissements du SSA en Ile de France (HIA parisiens, IRBA, CTSA, SPRA, Cetima), tous les établissements du Service pourront à terme profiter de ce partenariat.

ARMÉES D'AUJOURD'HUI

BSPP : deux siècles d

Créée par Napoléon en 1811, la Brigade de sapeurs-pompiers de Paris fête son bicentenaire. Sa mission : protéger les personnes et les biens. Sa devise : Sauver ou périr.

BSPP

Juillet 1810. Un incendie ravage l'ambassade d'Autriche à Paris, faisant près de 120 morts. Dix jours plus tard, Napoléon 1er crée une brigade de sapeurs-pompiers chargée de veiller à la protection de ses palais. Suivra un décret impérial le 18 septembre 1811, qui fixe le principe d'un corps à caractère militaire. Le Bataillon des sapeurs-pompiers de Paris est né. *« L'idée d'une militarisation des sapeurs-pompiers était judicieuse, puisqu'ainsi l'empereur assurait la loyauté des hommes à la puissance publique »*, explique le capi-

ans le feu de l'action

JULIEN PICHOT

A gauche : 1921. Des sapeurs-pompiers tentent d'éteindre un incendie aux magasins Le Printemps, à Paris.

A droite : 2010. Les moyens techniques ont évolué et les actions de la BSPP se sont diversifiées. Outre les incendies, les militaires interviennent dans le cadre de secours à la personne et d'accidents en tout genre.

taine Emmanuel Ranvoisy, officier spécialiste conservateur de la Brigade.
En 1859, Paris passe de 12 à 20 arrondissements. Le bataillon devient régiment. Les casernes se modernisent, de nouveaux bâtiments sont construits et la révolution industrielle impose ses marques. *« A la fin du XIXe, Paris est la capitale la mieux organisée dans la lutte contre les incendies, et la plus moderne. C'est l'âge d'or du service d'incendies parisien ! »,* ajoute le capitaine Ranvoisy. Première grande révolution, la traction hippomobile, qui apparaît avec l'invention de la pompe à vapeur, à ■■■

laquelle on ajoute des échelles. Entre 1900 et 1905, ces voitures à cheval sont peu à peu remplacées par les engins à propulsion électrique puis par les voitures à moteur à explosion. *« A la veille de 1914, le régiment est à la pointe de la modernité. Plus d'une vingtaine de casernes, relayées par des petits postes spécialisés dans les départs de feu, sont réparties dans la capitale. »* Entretemps, le baron Haussmann a fait élargir les voies, offrant de nouvelles perspectives à la BSPP, notamment grâce au réseau de distribution de l'eau en sous-sol. Depuis 1870, l'installation du réseau télégraphique permet en outre à la population d'appeler les secours bien plus rapidement.

Pendant la Grande Guerre, 1 200 pompiers demandent à être envoyés sur le front. Pour les remplacer, le ministère fera appel aux réservistes. *« Les postes de secours mobiles se sont développés pour traiter l'urgence sur place et les pompiers sont formés aux premiers soins. »* En juin 1940, alors que les Allemands entrent dans Paris, un réseau de résistance se constitue au sein du régiment. *« Le réseau Sécurité parisienne a été très impliqué au moment de la Libération »*, souligne le capitaine. En 1967, le régiment devient brigade, et son champ d'action s'ouvre à l'ensemble de la Petite Couronne dès 1968.

BSPP

Clermont-Ferrand, juillet 1940. Revue du bataillon de marche des sapeurs-pompiers par le général de Lattre de Tassigny.

Des missions très variées

Aujourd'hui, les 8 500 sapeurs-pompiers interviennent sur une zone de 760 km², regroupant Paris et les trois départements de la Petite Couronne (Hauts-de-Seine, Seine-Saint-Denis et Val-de-Marne), où vivent sept millions d'habitants. En 2010, la BSPP a réalisé 500 000 interventions. Et les missions des militaires se sont diversifiées : secours à personne, incendies, accidents technologiques, interventions diverses (fuites d'eau, matériaux menaçant de chuter…). Le cadre d'intervention des sapeurs-pompiers de Paris s'inscrit aussi dans des univers trés opposés, du sommet de la tour Eiffel au souterrain du métro. Il intègre le tissu technologique urbain des grandes mégapoles : 2 000 kilomètres d'égouts, 2 300 de canalisations de gaz et 250 de métro et de RER. Les sapeurs-pompiers voient leur métier évoluer. *« Outre la lutte contre le feu, le sauvetage et le secourisme, nous devons désormais faire face aux risques émergents,* explique le capitaine Ranvoisy. *C'est pourquoi nous formons des spécialistes des risques nucléaires, radiologiques, bactériologiques et chimiques (NRBC) ou d'autres pour les milieux périlleux. »*

Un seul matériel a traversé les siècles : l'échelle à crochet, utilisée depuis 1825, et dont l'efficacité n'est plus à prouver. La mission des sapeurs-pompiers, elle aussi, est immuable : ils veillent et veilleront toujours sur Paris et sur les Parisiens. ■

Domitille Bertrand

3 questions au général Gilles Glin, commandant la Brigade de sapeurs-pompiers de Paris ■

BSPP

Comment s'inscrit l'action de la BSPP dans la sécurité de la ville de Paris et de la région Ile-de-France ?

La BSPP remplit sa mission de protection des personnes et des biens en incluant les risques et les menaces : secours à personne, lutte contre les incendies, catastrophes (en collaboration avec la police, les services médicaux d'urgence, les associations de secouristes). Dans le cas de catastrophes majeures, des demandes de moyens en hommes et en matériels supplémentaires sont adressées à la zone de défense de l'Ile-de-France. En matière de sécurité et de menace terroriste, le préfet de police de Paris coordonne l'ensemble des actions de secours.

Dans une société marquée par l'individualisme, la jeune recrue de 2011 se retrouve-t-elle dans la devise Sauver ou périr ?

On n'entre pas à la BSPP par hasard. Il s'agit d'une démarche volontaire. Nos jeunes recherchent la rigueur, la discipline, l'engagement physique et moral. Ils savent, en choisissant ce métier, qu'ils devront s'impliquer totalement au profit des populations qu'ils servent. Ils en connaissent les risques, qui peuvent aller jusqu'au don de la vie.

Quel est l'impact de la dynamique de modernisation des armées sur la Brigade ?

La BSPP est très vigilante quant à l'évolution de son environnement, ceci afin d'apporter la meilleure réponse possible aux demandes de secours des populations. Dépendant de l'arme du Génie, la Brigade a bien évidemment été impactée par la modernisation des armées, notamment en ce qui concerne ses structures : nous recherchons l'efficience dans l'emploi des crédits. Une des solutions vise notamment à réarticuler la composante logistique de la Brigade en lui faisant adopter un format plus concentré, tout en préservant la « qualité de prestation ».

ARMÉES D'AUJOURD'HUI

Premier de cordée en milieu périlleux

Acrobate du sauvetage et spécialiste des interventions délicates en altitude ou en profondeur, Nicolas Lordel est sergent au Groupe de recherche et d'intervention en milieu périlleux (Grimp). Portrait…

Nicolas Lordel n'est pas très loquace et l'exercice de l'interview lui est plutôt difficile, même s'il s'efforce de le nier: *« J'ai l'habitude, les médias sont souvent tournés vers nous. La semaine dernière encore, nous avons accueilli une grande chaîne de télévision »*. A 32 ans, ce sergent chez les sapeurs-pompiers de Paris affiche un regard bleu-cendre et un nez esquinté de boxeur. Ce matin-là, il débute le premier round de la journée: un exercice « de routine » d'hélitreuillage dans le parc de Saint-Cloud. Coiffé d'un casque, harnaché d'un baudrier, de mousquetons et de cordes, Nicolas a l'allure d'un alpiniste de haute montagne. Et pour cause, il fait partie du Grimp, le Groupe de recherche et d'intervention en milieu périlleux. Ces acrobates du sauvetage sont les spécialistes des interventions délicates en altitude ou en profondeur. Au sommet d'un édifice ou dans les tréfonds des catacombes, leur concours est réclamé lorsque la situation dépasse le cadre des capacités traditionnelles des pompiers. Par exemple, lorsque l'état de la victime nécessite une évacuation par hélitreuillage ou par brancardage le long de la façade d'un immeuble. A la caserne d'Issy-les-Moulineaux, leur quartier général, ils ne sont que 54 spécialistes comme Nicolas pouvant être appelés à intervenir sur un secteur qui couvre l'ensemble de l'agglomération parisienne et sa Petite Couronne. Basés non loin de l'héliport de Paris, ils sont susceptibles d'être héliportés en temps record sur le lieu d'un sinistre. *« Aujourd'hui, c'est peut-être 15 % des sorties des pompiers qui sont consacrées à la lutte contre un incendie. Le reste se partage entre le secours aux personnes et aux biens, aux victimes d'accidents ou de catastrophes naturelles. Et puis pour les interventions plus délicates, il y a nous »* ajoute Nicolas.

A l'évocation d'« unité spéciale », il grimace et récuse l'intitulé, tout comme celui de « notoriété ». Pourtant, lui et ses hommes assurent régulièrement le spectacle auprès des touristes et des passants alors qu'ils s'entraînent à escalader la tour Eiffel ou un édifice du quartier d'affaires de la Défense.

Nicolas Lordel est un enfant du Grimp. Il rejoint les rangs des sapeurs-pompiers à 20 ans. *« Pour faire partie du Grimp, il faut au moins quatre ans d'ancienneté à la brigade et subir ensuite une sélection éprouvante. Ancien pompier volontaire, j'avais déjà les qualifications et les diplômes requis pour prétendre intégrer l'unité. J'ai donc été directement muté à la caserne d'Issy. J'étais une exception, le plus jeune, un enfant presque. »* A ce jour, il est le plus aguerri des hommes du Grimp et considère sans amertume la jeune génération de pompiers qui prendra sa relève: *« J'ai un défaut, je leur parle souvent des anciens et de leurs enseignements. Mais c'est parce que j'aime par-dessus tout transmettre mon expérience. »* Une expérience faite de départs précipités, de sauvetages en catastrophe, de claps de fin heureux ou moins heureux: *« Certaines images impriment encore ma mémoire. Oui, elles se rappellent à moi de temps à autre. »* Un jour, le sergent Lordel est dans les entrailles d'un tunnel en chantier d'une autoroute en proie aux flammes, le lendemain au sommet de la basilique du Sacré-Cœur pour évacuer une personne intransportable par les voies habituelles. *« Je ne sais jamais à l'avance de quoi demain sera fait et c'est pour cette raison que je me suis engagé dans cette spécialité. Ce n'est ni par passion pour l'escalade, ni par goût du risque »*, avance Nicolas.

« Je ne sais jamais à l'avance de quoi demain sera fait et c'est pour cette raison que je me suis engagé au Grimp. »

Depuis le début de l'année 2011, le Grimp parisien totalise déjà 135 interventions. ■

Grégoire Chaumeil

Casqué, harnaché d'un baudrier, de mousquetons et de cordes, Nicolas vient d'être hélitreuillé, un simple exercice de routine pour ce membre du Grimp.

GRÉGOIRE CHAUMEIL/DICOD

FONDS ALLEMAND/ECPAD

Belgique, mai 1940 : annonce de la reddition des forces belges
Une habitante de Bruxelles apprend par le journal la capitulation de son armée le 28 mai 1940. Après la drôle de guerre de septembre 1939 à mai 1940, marquée par le peu de combats au sol, l'armée allemande passe à l'offensive le 10 mai. Elle envahit la Belgique, les Pays-Bas, le Luxembourg et la France. Très vite, les armées alliées sont encerclées à Dunkerque… Ce cliché fait partie d'un fonds photographique d'images de propagande qui présentent la Campagne de l'Ouest, du 10 mai au 22 juin 1940, vue du côté allemand.

Du secret de la stratégie...

...à la stratégie des fuites

Indispensable à la stratégie de la guerre et dans la diplomatie, le secret doit être jalousement protégé. Parfois instrumentalisé, il reste une arme à manier avec précaution.

Le secret est une arme plus ancienne que l'épée. Comme elle, cependant, il présente un double tranchant. Consubstantiel à la guerre, et donc à la stratégie, il est indispensable à la protection des troupes et des matériels, à l'accroissement des marges de manœuvre des chefs et à la sauvegarde de l'effet de surprise. Il est une condition nécessaire, bien que non suffisante, de la victoire. De Sun Zi à Mao Zedong, de Richelieu à Napoléon, tous les grands stratèges et stratégistes ont souligné l'impérieuse nécessité de protéger les secrets de son camp tout en traquant ceux de l'adversaire. Au service d'une stratégie intégrale, le secret se justifie tout autant à l'échelon politico-diplomatique auquel le militaire est subordonné. On ne saurait concevoir de processus de décision sans discrétion, ni de diplomatie efficace sans un recours ponctuel et parfois prolongé au secret. La restauration de la confiance, indispensable aux belligérants désireux de mettre un terme à leur conflit, est souvent à ce prix.

Pour autant, le secret a toujours généré ses propres antidotes. Dans une démocratie en guerre où s'exerce un certain degré de censure, les velléités pour le contourner sont nombreuses : le *Canard Enchaîné* n'est-il pas né en pleine Première Guerre mondiale, contre les excès de la censure et de la propagande d'Etat ? La presse exerce un rôle autant privilégié que redouté à cet égard. Mais les journalistes ne sont le plus souvent que des intermédiaires. Toutes les administrations gouvernementales sont en effet traversées, de la base jusqu'au sommet, par des rivalités internes, des divergences, voire des oppositions sur les moyens mis au service d'une stratégie, quand ce n'est pas sur les buts eux-mêmes. L'une des expressions classiques de ces contradictions bureaucratiques réside dans l'instrumentalisation des fuites d'informations secrètes à la presse. Cette stratégie des fuites peut être mise aussi bien au service de la guerre – pour torpiller par exemple un processus de paix auquel on est opposé, accroître ses gains dans la négociation et/ou renforcer sa position dans son propre camp politique – que de la paix, pour accélérer la fin d'une guerre que l'on juge contre-productive et injuste. Parce qu'elle a cristallisé des oppositions irréductibles, la guerre du Vietnam offre maintes illustrations de cette ambivalence. L'existence de filières de contact américano-vietnamiennes secrètes précédant ou accompagnant les négociations officielles a parfois été ébruitée dans la presse à l'initiative de certains membres de l'administration qui croyaient encore en la possibilité d'une victoire militaire. A l'inverse, sans la détermination de Daniel Ellsberg, expert du Vietnam au Pentagone rallié au parti des opposants à la guerre, les célèbres *Papiers du Pentagone* n'auraient sans doute jamais été divulgués à la grande presse américaine, et le public américain n'aurait rien su des incohérences et des mensonges de l'administration Johnson sur sa politique vietnamienne.

CHRISTOPHE FIARD/DICOD

PIERRE JOURNOUD
chargé d'études à l'Institut de recherches stratégiques de l'Ecole militaire (Irsem).

Syndrome du Watergate

Mal dosé, confondu avec l'objectif alors qu'il doit rester un moyen, le secret peut alors provoquer de graves effets en retour. Les « actions clandestines », « armées secrètes » ou « guerres secrètes » que l'on a vu fleurir sur tous les continents, spécialement depuis la décolonisation et la guerre froide, ont nourri l'indignation et donné naissance au syndrome du *Watergate*, du nom de la grande affaire politico-médiatique qui a fait chuter le président Nixon en 1974. A l'ère informationnelle, marquée par une tension permanente entre l'occulte et la transparence, dont WikiLeaks est le dernier avatar, on comprend tout l'intérêt que revêt le secret lorsqu'il est mis au service d'une stratégie cohérente. A défaut, l'histoire récente témoigne qu'il peut être fatal au pouvoir qui serait tenté d'en abuser. ■

JEAN-CLAUDE JAEGER

LES SOLDATS DU FEU Histoire illustrée des sapeurs-pompiers

A l'occasion du bicentenaire de la création par Napoléon 1er, du bataillon des sapeurs-pompiers de Paris, les éditions Pierre de Taillac publient *Soldats du feu – histoire illustrée des sapeurs-pompiers*, d'Eric Deroo. A travers plus de 400 photographies inédites provenant de la collection de son père Raymond Deroo, ancien conservateur du musée de la brigade des sapeurs-pompiers de Paris, cet ouvrage nous fait revivre le quotidien et les exploits de ces héros anonymes d'hier et d'aujourd'hui. De la création du bataillon de sapeurs chargé des pompes à incendie de la ville de Paris, en 1811, à la menace terroriste contemporaine, des incendies de la Commune aux guerres mondiales et aux sinistres gigantesques qu'elles ont provoqués, l'auteur revient sur la fabuleuse aventure de ces soldats du feu, qui ont juré de Sauver ou périr. Un livre passionnant.

Eric Deroo, éd. Pierre de Taillac, coll. de photographies du commandant Deroo, 239 p., 35€

LES AVISOS A69

Dix-sept avisos du type A69 sont entrés en service dans la marine nationale entre 1976 et 1986. Armé pour la lutte anti-sous-marine par petits fonds, l'A69 fut conçu à l'origine pour sécuriser, aux approches de Brest, les appareillages et les retours de patrouille des sous-marins nucléaires lanceurs d'engins (SNLE) basés à l'Ile Longue. Bâtiment particulièrement endurant, ses missions ne tarderont pas à se diversifier, de la surveillance des zones de pêche à la lutte contre les pirates et narcotrafiquants. Rebaptisés « patrouilleurs de haute mer » en 2009, les derniers d'entre eux resteront en service jusqu'en 2020. Patrick Maurand et Jean Moulin signent ici un bel album retraçant l'histoire et les caractéristiques de chacun de ces avisos sur lesquels, depuis 1976, de nombreux marins ont un jour navigué.

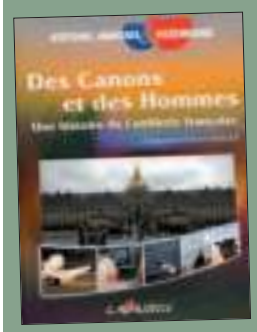
Patrick Maurand et Jean Moulin, Marines Editions, 220 p., 45 €

BOMBARDER POUR VAINCRE. Puissance aérienne et coercition dans la guerre

Bombing to win, publié aux Etats-Unis en 1996, traduit en français par le lieutenant-colonel de l'armée de l'air Jean-Patrice Le Saint est un livre magistral qui analyse l'impact du bombardement stratégique. L'auteur Robert A. Pape propose une conceptualisation rigoureuse des ressorts de la coercition afin d'orienter le choix des décideurs. S'il évoque le rôle des armées de terre et de mer, il se focalise sur l'emploi de la puissance aérienne. Elle est pour lui, de tous les instruments militaires, celui qui offre le meilleur potentiel coercitif, à condition toutefois de l'employer à bon escient, en renonçant aux chimères du bombardement stratégique. A travers l'étude de 33 campagnes aériennes, l'auteur établit le rôle déterminant de l'interdiction du champ de bataille et de l'appui aérien rapproché. Même si certaines de ses conclusions ne manqueront pas de susciter le débat, ce livre est l'un des grands classiques de la stratégie aérienne.

Robert A. Pape. Traduit de l'américain par le lieutenant-colonel Jean-Patrice Le Saint, éd. La documentation française, coll. Stratégie aérospatiale, 427 p., 24€

DES CANONS ET DES HOMMES Une histoire de l'artillerie française



Ecrit par un artilleur de métier, cet ouvrage est une vaste synthèse dont la première partie couvre l'histoire de l'artillerie, depuis la prise de Castillon par les troupes royales en 1451, jusqu'aux récents déploiements des canons Caesar en Afghanistan. Une deuxième partie décrit l'organisation des différentes subdivisions d'armes et précise les évolutions tactiques et techniques des artilleries de montagne, de marine, aérienne ou parachutiste. Une dernière partie, plus particulièrement dédiée aux jeunes artilleurs, résume les faits d'armes, les traditions et l'héritage des unités actuelles.

Colonel (er) Patrick Mercier, éd. Lavauzelle, 389 p., 27€

CHRONOLOGIE COMMENTÉE DE LA PREMIÈRE GUERRE MONDIALE

Du 28 juin 1914, jour de l'assassinat de l'archiduc héritier d'Autriche, au départ de France du président Wilson, le 29 juin 1919, cet ouvrage restitue, jour après jour, sur tous les fronts, tous les épisodes de la Première Guerre mondiale. Rédigée par le lieutenant-colonel Rémy Porte, enseignant-chercheur à l'Ecole supérieure des officiers de réserve, cette chronologie a été conçue selon lui comme *« un outil permettant aux étudiants et aux passionnés d'explorer l'extraordinaire diversité de la Grande Guerre »*. L'analyse de chaque journée est complétée par de nombreuses citations tirées de mémoires, de correspondances ou de journaux d'époque. Cet ouvrage vient de recevoir le prix "Général Muteau" de l'académie des sciences morales et politiques

Rémy Porte, éd. Perrin, 645 p., 26 €