Salle opérationnelle.

Sécurité informatique, Open-source et technologies intranet

Xavier Guimard

Colonel
sous-directeur des applications de commandement
au service des technologies
et des systèmes d'information de la sécurité intérieure

1993, l'entrée en Gendarmerie

Je suis polytechnicien, promotion 1990, sortie en 1993 et j'ai choisi la gendarmerie.

Tout d'abord à l'École polytechnique, j'ai opté pour la mécanique des fluides qui a priori n'a rien à voir avec les missions de la gendarmerie. Mais avant d'intégrer Polytechnique, j'étais un cavalier de haut niveau et je participais aux compétitions équestres. En première année d'X, j'ai découvert les armées et notamment la Gendarmerie grâce à un cadre de contact qui était un officier de l'Arme. J'ai ainsi découvert les valeurs des officiers et les possibilités offertes en début de carrière. J'ai donc intégré la gendarmerie dans le but de devenir cavalier dans un premier temps.

L'EOGN était une école aux bâtiments austères, d'apparence abandonnée et dirigée à l'époque par un général en fin de carrière. Pour les officiers arrivant en troisième année, le rattrapage en droit était intense et ma formation d'ingénieur mise en sommeil. À l'issue de l'EOGN, mon choix s'est naturellement porté sur la Garde républicaine pour allier mon métier à ma passion pour l'équitation.

1993-1998, l'expérience du commandement à la Garde républicaine

À la Garde, j'ai commandé un peloton à la caserne Carnot à Vincennes, puis un escadron aux Célestins dans Paris. En 1997, la gendarmerie a renoué avec les patrouilles équestres dans Paris.

La visite du Pape Jean-Paul II sur le site de Longchamp a ouvert la voie à la réintroduction du cheval en service d'ordre à Paris, mission abandonnée depuis 1934. Initialement, la mission était connexe : surveillance des bois et recherche du renseignement en profondeur. Le général Föllmi qui commandait la zone de gendarmerie de Paris m'a alors confié une mission simple : « se rendre indispensable ». Au final la mission s'est bien révélée essentielle voire indispensable car nous avons pu escorter plusieurs centaines d'ambulances. Les gens s'écartaient naturellement à l'approche des chevaux. Nous avons également ouvert la route pour les autorités car les motards, en raison de l'afflux du public, n'y parvenaient pas.

Après 4 années à la Garde, en 1998, j'ai rejoint, pour la commander, la compagnie de gendarmerie départementale de Saint-Germain-en-Laye. Un parcours classique pour un officier de gendarmerie.

2000, le choix de la spécialité SIC

La carrière d'un officier s'articule autour de postes en états-majors, à la direction générale et sur le terrain. Après le temps de commandement en compagnie, il fallait choisir une voie. Avec mon cursus scientifique, plusieurs opportunités étaient possibles : criminalité, informatique, télécommunications, etc. Pas forcément décidé à me lancer dans la spécialité des systèmes d'information et de communication, c'est par mon commandant de groupement, le colonel Carmichaël, que je me suis intéressé à la matière, notamment à la sécurité informatique. Alors capitaine, je pouvais encore intégrer un cursus de formation supérieure. Et même si le grade de chef d'escadron m'était promis rapidement, l'avancement me barrait cette voie pour des raisons statutaires. Les cours de l'X sur ce domaine n'avaient pas suscité un grand intérêt, même si je programmais un peu à titre personnel. La sécurité informatique avait un attrait et m'ouvrait de nouvelles perspectives de carrière. J'ai déposé ma candidature pour l'enseignement militaire supérieur et technique en vue d'obtenir un mastère en sécurité informatique à Télécom Paris. De forma-

La bureautique fait partie du quotidien des unités de la gendarmerie depuis le milieu des années 1990.

Page d'acueil d'Agorha en 2016.

tion militaire, j'étais surpris que les cours portent uniquement sur la défense contre un ennemi qui n'est pas identifié alors qu'il n'est pas envisageable de former un militaire à se défendre sans apprendre l'attaque ne serait-ce que pour la comprendre. J'ai donc cherché un stage me permettant de voir l'autre côté du miroir. Au cours de celui-ci j'ai participé à des intrusions informatiques aux côtés de l'équipe d'audit de France Telécom. Mon statut de gendarme me permettait d'obtenir la confiance nécessaire car les audits portaient sur des services innovants internes et France Telecom n'avait nulle envie de voir ces informations arriver à la concurrence. Mon mémoire consistait à réaliser des maquettes d'attaques informatiques pour sensibiliser les dirigeants à la sécurité.

2001-2005, la grande réforme de l'informatique de la gendarmerie

En fin de formation, en octobre 2001, le mastère en poche, je suis arrivé à Rosny-sous-Bois comme adjoint de la section sécurité du bureau conception coordination à la sous-direction des télécommunications et de l'informatique de la direction générale (SDTI). Une petite section à 6 dont 3 personnels s'occupaient du chiffre. Pour la Gendarmerie, c'était le tout début de la sécurité informatique car jusque-là seul le chiffre était géré. Les réseaux IP en Gendarmerie étaient tout juste opérationnels : avant cela les systèmes fonctionnaient en X25.

À mon arrivée, il existait une cellule Intranet composée de 4 personnes. Pour diverses raisons, j'ai œuvré à l'interconnexion avec le nouveau réseau interadministration AdER et donc j'ai été amené à travailler avec le chef de cette cellule, le capitaine Marc Boget (aujourd'hui colonel). Le général Brachet, SDTI et avant-gardiste, a été l'initiateur de la nouvelle gouvernance de l'informatique qui intégrait entre autres la sécurité dès le début des réflexions. C'est lui qui a introduit les raisonnements militaires dans l'informatique de la gendarmerie. Nous avions des envies et des besoins.

Internet devenant indispensable au fonctionnement des unités, une solution palliative avait été trouvée consistant à installer dans toutes les unités une connexion Internet dédiée. Outre l'aspect onéreux de la solution, diverses contraintes notamment juridiques nous poussaient à rendre ce service via l'Intranet qui allait être déployé à compter de 2005. Toutefois le raccordement d'un Intranet véhiculant des données sensibles et de surcroît connecté à celui de la défense nécessitait un haut niveau de sécurité. Nous partions de très loin… Sous l'impulsion du général Brachet, nous avons réalisé un véritable travail d'état-major militaire pour répondre à tous les besoins et contraintes. Le colonel Dégez a donc réorganisé le bureau conception coordination en créant deux sections : l'une concernée par l'architecture et les systèmes, l'autre pour la veille et la sécurité informatique, mettant en œuvre l'une des conclusions de ce travail.

Au lieu de s'appuyer sur les modèles classiques (qui sont devenus les ISO 27000 et suivants) qui, en gros, listent les actions à réaliser sans offrir d'alternatives en cas de manque de moyens, nous avons choisi de comparer notre objectif à atteindre à la défense d'une place. Pour reprendre le raisonnement militaire et en caricaturant, une ville du haut Moyen-Âge n'est pas implantée par hasard, mais sur des choix de soutenabilité essentiellement économique. Dans un second temps, sa défense s'effectue par la mise en œuvre de remparts. L'histoire de l'architecture militaire, nous a conduit à reproduire le schéma « Vauban » : un militaire « architecte »

est chargé de déplacer et concevoir à nouveau la ville pour obtenir un compromis entre soutenabilité économique et défense et un autre militaire est chargé d'assurer sa défense. La section architecture du bureau conception coordination a donc créé un système défendable, tout en restant à la recherche constante de compromis. La section de la sécurité va défendre l'architecture en place. En procédant de telle sorte, à coûts contraints, nous avons élevé la sécurité tout en diminuant les effectifs de la filière SIC de près d'un tiers et en préservant la qualité de l'engagement des personnels télécommunications-informatique sur le terrain. C'est donc en intégrant les raisonnements militaires que nous sommes arrivés à une architecture sécurisée. Intégrer la sécurité dès le début du projet conduit à réduire les coûts globaux.

En 2002, j'ai été nommé chef de la section architecture des systèmes, héritière de la cellule intranet à l'effectif de quatre militaires. Cependant le chef de la section sécurité n'était pas encore affecté, j'ai en pratique commandé les deux sections pendant trois mois.

Un autre levier très important de la sécurité dans le temps est de contenir les coûts. Nos travaux nous ont conduit à imaginer une politique visant à rétablir en permanence les conditions de la concurrence. En nous appuyant sur les principes alors oubliés des premières externalisations du ministère de la Défense : la transférabilité et la réversibilité (réinternalisation), nous avons inventé un modèle nommé « modèle des briques » qui empêchait l'interdépendance des projets pour qu'aucune mise en concurrence ne soit biaisée par l'existant. Adossé à une forte modularité ; ce modèle a rendu les chefs de projet clients des services offerts par la « nouvelle ville ». La logique avait changé, l'installation d'un projet n'était plus un nouveau silo dans l'architecture. Mais il est intégré à la citadelle et bénéficie de ses nombreux services mutualisés et sécurisés. Progressivement, les vieilles applications restées dans la « vieille ville » ont disparu pour un système d'information à la fois global et modulaire.

En 2003, cette stratégie globale a été clairement définie par le général Brachet et tous les chefs de projet travaillent depuis dans le même sens.

Grâce à la LOPPSI, la gendarmerie a obtenu des fonds supplémentaires, notamment pour moderniser certaines applications. Les projets se nomment TAJ (Traitement des Antécédents Judiciaires), PULSAR, Agorh@ (Application de Gestion de l'Organisation et des Ressources Humaines).

Sur un plan plus technique, la SDTI a lancé Proxim@ (c'est le socle de notre système d'information qui supporte les applications métiers, bref, le nom de notre ville fortifiée). Différents incidents administratifs nous ont conduit fin 2004 à décider d'internaliser la solution.

Le « modèle des briques » obligeait notamment l'utilisation de protocoles standards et libres de droits ou propriété de la gendarmerie. Or, les logiciels libres respectent les standards en plus d'être gratuits. Vers 2005, le ministère des Finances a analysé ainsi cet aspect pour des serveurs Java J2EE et a constaté un fonctionnement équivalent pour un coût très réduit notamment sur les coûts récurrents. La même démarche appliquée à d'autres secteurs a poussé la gendarmerie à employer massivement les technologies libres.

Un autre levier de performance est l'internalisation des risques. Par exemple, pour le projet de la carte professionnel, nous avons modularisé à

Couverture de magazine.

l'extrême en intégrant le risque de l'assemblage : un marché pour l'acquisition des cartes à puce qui répondent strictement aux standards, un autre marché pour l'acquisition des lecteurs de cartes à puce répondant aux mêmes standards dans la même logique et quelques marchés complémentaires pour adapter un logiciel libre et produire les documents légaux. Au final, ce projet détaché en briques n'a coûté que 2,5 M€ alors qu'un autre ministère régalien, en recherchant une solution complète, a déboursé plus de 7 M€ pour une simple maquette !

À partir de 2005, « Open source : la Gendarmerie ouvre la route »

L'arrivée en gendarmerie de la suite bureautique d'Open-office n'est qu'une conséquence de cette politique de rationalisation et Microsoft a lui-même déclenché cette migration.

Véhicule LAPI avec caméra et TIE.

Ainsi, la solution de s'appuyer sur une norme pour les documents bureautiques était dans les cartons. en 2004, la politique de vente de logiciels de bureautique a évolué chez Microsoft entraînant pour nous un surcoût (+ 120 € par ordinateur) soit à budget constant une diminution du parc. Le nombre d'ordinateurs était alors des plus sensibles et constituait l'un des indicateurs du tableau de bord du ministre. Le colonel Labbé, alors chef du bureau de la gestion, nous a exposé alors ses difficultés un matin autour d'un café. Nous lui avons parlé alors sans trop de conviction de notre vue, Open-office, suite bureautique gratuite respectant le standard n'était pas alors aussi abouti qu'aujourd'hui. Il nous a demandé alors de l'installer sur son poste pour essayer. Quelques jours après, sa conclusion était simple : j'y suis arrivé sans difficulté, banco ! Ce choix a finalement été validé par le directeur général, non pas sur le seul périmètre des unités élémentaires, mais, suite à la maxime « pas de village gaulois », il nous a donné l'ordre de généraliser Open-office à tous les ordinateurs de la Gendarmerie !

Les réticences ont été nombreuses à l'exception du terrain qui possédait des outils adaptés à la rédaction de procédures. La communauté IC@RE alors été fondée pour fournir les imprimés numériques nécessaires à la rédaction de procédures en lieu et place des macros words jusqu'alors utilisées pour leur rédaction. Ainsi, on n'amenait pas Open-office, mais la communauté IC@RE. Pour implanter le produit, il a fallu faire un peu d'intelligence économique en contrôlant habilement les fuites d'information. En 2005, 70 000 postes de travail ont ainsi été équipés.

La communication vers le terrain a été orientée par le biais de cette communauté IC@RE avec la reconnaissance des développeurs bénévoles qui fournissaient depuis de nombreuses années les logiciels réellement utilisés sur le terrain. Nous avons par ce biais obtenu l'adhésion des gendarmes. Nous avons fait migrer les applications les unes après les autres. Linux est venu en dernier. Quand le gendarme devait rédiger une procédure, il allait vers IC@RE. Windows ou Linux n'avait plus d'importance. Les états-majors étaient plus réfractaires au changement. Historiquement, leurs macros Excel avaient été réalisées par des gendarmes auxiliaires et scientifiques du contingent et n'étaient souvent plus maintenues. C'était, par conséquent, plus simple de convaincre les plus réfractaires d'abandonner leur solution et de migrer vers les nouveaux outils. Pour autant, pour pallier certaines carences, nous avons formé, en région, quelques développeurs en PHP-MySQL.

Pour contrer nos avancées et migrations vers le monde libre, les représentants de Microsoft ont usé de nombreuses manœuvres particulièrement déloyales. Je me souviens de l'une d'entre elles, qui les a conduits à rencontrer le général Espinasse, successeur du général Brachet, et à dénoncer les propos d'un officier et d'un sous-officier à l'encontre de Microsoft lors d'un salon LINUX. L'officier mis en cause n'était autre que moi-même ! Sauf que cette semaine là, j'étais au ski !

Autre anecdote, ces mêmes dirigeants ont également rencontré le directeur général de la gendarmerie pour dénigrer le travail de la SDTI et le prévenir d'un échec assuré. Nous avons aussi été audités par le contrôle général des armées à la suite d'une dénonciation de cette même société pour non-paiement des licences Microsoft, mais nous avons pu prouver que nous avions payé 102 % de nos licences. Rien n'y a fait, nous étions sur la bonne voie.

L'année 2005 fut riche en avancées significatives dans le domaine de l'informatique. Le portail intranet gendarmerie a été enrichi d'un nouveau service d'annuaire web permettant la consultation et la mise à jour d'informations concernant l'ensemble des unités et des personnels de l'institution. Avec visualisation du lien entre chaque personnel et son unité d'affectation.

L'application courrier est la première dont les droits et les comptes sont basés sur l'annuaire web et ainsi créés automatiquement.

La messagerie organique offre un système de transmission comparable aux centres de transmission qui émettaient jusqu'alors les messages via Transwin.

Le SSO, service d'authentification unique destiné aux applications métiers a constitué une première puisque c'est la gendarmerie qui l'a publié en Open-source.

Le réseau Saphir 3G a été déployé dans la même période : toutes les brigades de métropole disposaient d'intranet (et un an après celles de l'outre-mer).

En 2006, étape importante de la démarche initiée en 2002, Internet est arrivé sur le poste de travail. Tous les critères ont été respectés et nous avons récupéré au passage les 6 000 ordinateurs alors dédiés à Internet. Beaucoup de contrôles ont été effectués par les experts du domaine du ministère de la Défense et de l'Agence Nationale de Sécurité des Systèmes d'Information (l'ANSSI). Aucune faille significative résiduelle n'a été détectée.

En 2007, nous avons pris la décision de faire migrer la majorité des ordinateurs sous Linux et d'abandonner progressivement XP au lieu de basculer sous Windows Vista qui posait de nombreux problèmes. D'autres attaques ont alors vu le jour, sans influence sur nos choix stratégiques. À notre arrivée au ministère de l'Intérieur, nous avions alors un système efficace et peu coûteux.