LE RENSEIGNEMENT, NERF DE LA GUERRE ÉCONOMIQUE

Interview de
BERTRAND DE TURCKHEIM (78)
cofondateur d'Axis & Co

Bertrand de Turckheim (78) a fait de l'intelligence économique son métier après une carrière militaire. Dans son activité s'entremêlent techniques de renseignement militaire et connaissance du privé, deux précieux atouts pour faire face à la réalité de la guerre économique.

Quel est votre parcours ? Comment en êtes-vous venu à travailler dans l'intelligence économique ?
À la sortie de l'X, j'ai choisi de rester dans l'armée. J'ai servi vingt-cinq ans dans l'institution militaire, avec une affectation de cinq ans à la DGSE et deux affectations à la Direction du renseignement militaire où j'étais l'équivalent d'un directeur des services informatiques. Entre les deux, j'ai effectué une scolarité à Télécom Paris dans le cadre de l'Enseignement militaire supérieur scientifique et technique. À la DGSE, j'étais conseiller technique du directeur des opérations à la fin des années 80. La problématique de l'informatique et des télécoms de terrain commençait à devenir intéressante. Aller à Télécom pour me mettre à jour sur ce volet était donc une opportunité à saisir. Dès que j'ai eu fini Télécom à Sophia Antipolis – dans la première promotion Eurecom – j'aurais dû poursuivre ma formation militaire, mais la Direction du renseignement militaire qui venait d'être créée par le général Heinrich, mon ancien patron à la DGSE, avait besoin d'un DSI. L'armée de Terre a accepté, moyennant un intermède de deux ans en Guyane pour reprendre contact avec le corps de troupe.

Avez-vous aimé le commandement militaire ?
Je recommence demain ! J'ai eu une carrière sur deux rails : un rail classique opérationnel et un rail technique et cette carrière s'est achevée avec le graal du commandement au 1er RPIMA à Bayonne au sein des Forces spéciales et finalement comme chef d'État-Major à Djibouti. Cela m'a donné une vraie compétence dans le domaine du renseignement, très orientée terrain au début, et après, quand j'ai rejoint la Direction du renseignement militaire, plus orientée sur la méthodologie et le traitement de l'information. Entre les deux, le général Heinrich m'a envoyé pendant neuf mois comme « tête de chaîne » du renseignement français en ex-Yougoslavie. Là, j'ai eu la chance de faire du renseignement en opération au sein des structures internationales, ONU puis Otan.

Qu'avez-vous fait après l'armée ?
J'avais envie d'avoir une expérience d'entrepreneur. J'ai donc quitté l'institution militaire et j'ai commencé une deuxième vie professionnelle, à nouveau grâce au général Heinrich qui était à l'époque au conseil de surveillance de Geos. C'était la première entreprise traitant de la problématique de sécurité et d'intelligence économique en France. Ils avaient besoin d'un directeur général et j'ai été recruté en 2004. L'activité couvrait la sécurité des expatriés (une partie importante du chiffre d'affaires), la sécurité de type gardiennage et l'intelligence économique que dirigeait Jean-Renaud Fayol. C'est avec lui que j'ai assez rapidement fondé Axis, comme *pure player* de l'intelligence économique.

Quel est votre cœur de métier ?
Jean-Renaud avait la compétence sur le volet investigation humaine tandis que j'apportais la dimension technique. Dans un premier temps, le volet technique devait garantir la confidentialité et la protection des informations de nos dossiers. Rapidement, j'ai renoué le contact avec des personnes croisées dans ma carrière militaire, notamment celui qui avait été notre RSSI à la DRM à la fin des années 90. Nous avons monté une compétence dans le domaine du *forensics*, ou plus exactement dans l'investigation digitale qui va des téléphones jusqu'au *darknet*, en passant par les ordinateurs et les systèmes informatiques, les menaces étant multiformes et allant de la fuite d'information dans un conseil d'administration d'une entreprise du CAC 40 à une tentative de racket d'une banque… Nous voulions avoir une approche beaucoup plus globale et être capables d'aller rechercher les traces et preuves de fraudes sur l'ensemble des outils digitaux.
Aujourd'hui nous sommes positionnés dans l'investigation humaine et digitale et la sûreté (malveillance) de l'information. Notre connaissance des techniques de *hacking* nous donne une compétence pointue dans l'analyse des possibilités d'attaque et des moyens de s'en protéger. En matière de sûreté de l'information, nous avons conçu et développé une solution sur des bases pragmatiques qui se sont révélées quasi conformes à l'instruction interministérielle n° 901 qui définit les contraintes ou les spécifications pour le traitement de l'information à diffusion restreinte. Cette solution, baptisée Sanctuaris, est déployée chez Orange et nous, nous sommes en cours d'homologation par l'ANSSI.

On retrouve des racines militaires, des techniques de terrain dans votre métier d'aujourd'hui…
Intelligence économique, c'est le terme anglais pour renseignement et il se trouve que les militaires font du renseignement par nécessité depuis toujours. Mais le renseignement c'est avant tout la nécessité de comprendre l'environnement avec lequel vous interagissez ; c'est l'intelligence de situation. La particularité depuis le rapport Henri Martre qui en avait posé les bases, c'est le développement d'Internet et la mondialisation. Une des difficultés réside dans le fait de développer ses activités dans des régions où le mode de travail n'est pas forcément celui du monde occidental. Au-delà de la fiche pays, il faut anticiper ce qui vous attend, notamment avec vos interlocuteurs et partenaires locaux.

En France, les entreprises sont-elles bien sensibilisées à ce sujet ou naïves ?
Je pense que ça évolue dans le bon sens. Nous avons défendu l'un des principaux acteurs français du luxe quand son principal concurrent est monté en force au capital. C'est un cas franco-français. Dix ans après, la situation s'est normalisée mais ça a été tendu. Notre client était très naïf, son adversaire beaucoup moins. L'intelligence économique, ce n'est pas que les opérations de fusion-acquisition même si le caractère brutal de ces dernières en donne une image guerrière. Nous faisons la distinction entre préventif et curatif. Le curatif, c'est typiquement l'enquête sur des fraudes notamment financières ou les diffusions d'informations confidentielles. En préventif, la *compliance* est aujourd'hui une vraie nécessité. Nous avons une partie conformité pour le KYC (*know your customer*) des banques. Il y a encore peu de temps, si vous envisagiez de développer vos affaires en Iran, il était indispensable de vérifier au préalable que toute personne impliquée de près ou de loin dans votre projet n'était pas dans les fichiers de l'OFAC (*Office of Foreign Assets Control*) de façon à vous éviter tôt ou tard des problèmes avec les Américains. Nous avons créé une structure en Suisse dans la diplomatie d'affaires pour poursuivre les affaires que nous avons renseignées et utiliser les contacts et le travail de connaissance du contexte.

> ***"C'est une nécessité de comprendre l'environnement avec lequel vous interagissez."***

Comment analysez-vous le cas des grandes affaires de rachat d'entreprises européennes par de grandes entreprises américaines concomitamment à des poursuites lancées par le DoJ ?
Il n'y a pas que les Américains qui le font mais ils ont la faculté d'utiliser un système juridique mondialement omnipotent. Ce sont des outils, parmi d'autres, mis à disposition par leur pouvoir politique. Il est donc toujours légitime de s'interroger quand une grande entreprise américaine rachète une entreprise européenne, mais la bonne posture doit être prise avant que l'agresseur ne se manifeste.

Y a-t-il un équivalent français ou européen à l'application extraterritoriale du droit américain ?
Aujourd'hui on peut se protéger de procédures en *disclosure* mais nous sommes quand même globalement ou naïfs, ou moins agressifs dans les affaires. Dans le cas de l'acteur français du luxe, l'attaque ne venait pas des États-Unis, mais il n'y avait aucune prise en compte de la protection des informations sensibles. Les choses évoluent…
Le problème c'est qu'on entend beaucoup parler des fraudes sur Internet et maintenant du volet influence mais on ne parle pas beaucoup du volet renseignement. D'une part parce que quand c'est bien fait, vous ne le savez pas, et si vous le découvrez, vous voulez éviter que cela se sache. Aujourd'hui, le bilan des attaques informatiques aux fins de renseignement est très mal connu. On connaît mieux le volet escroquerie, de la carte bancaire jusqu'aux *ransomwares* et aux attaques disruptives. Il faut protéger son information mais il faut envisager d'aller plus loin. Pour certains clients, →

nous avons des stratégies contre-offensives. Le contre-espionnage, qui constitue le troisième et ultime volet du renseignement, se décline en contre-intelligence économique, c'est à dire « hacker le hacker », mettre en place des stratégies « pots de miel, etc. ». C'est le volet le plus difficile car les adversaires sont des gens du métier du *hacking* ou de l'espionnage. Mais dans l'espionnage, les contre-espions sont les maîtres. Donc une stratégie de contre-intelligence économique est la stratégie ultime.

Pensez-vous possible que se pratique de l'espionnage dans les entreprises françaises ou européennes au profit du gouvernement américain ?

Si l'on parle de renseignement économique, je pense que ça relève du probable, voire du quasi certain surtout si on ne se limite pas aux Américains. En France, il y a une certaine naïveté vis-à-vis de la nécessité de se protéger. Les Anglo-Saxons, les Japonais sont bien plus conscients du fait que l'information dont ils disposent peut intéresser. Dans certaines de nos prestations, nous analysons l'environnement d'une personne uniquement à partir de sources ouvertes sur internet. Le *social engineering* vous permet en effet de construire un dossier d'objectifs, pour reprendre une terminologie militaire, qui dans un deuxième temps vous permettra de déjouer la vigilance de votre cible en utilisant certaines techniques. Le premier cercle autour de la cible n'a pas conscience du fait que des informations extrêmement banales qu'ils diffusent sur les réseaux sociaux peuvent être récupérées par des gens qui veulent attaquer, pour le renseignement ou la fraude. Il est donc indispensable que les dirigeants connaissent leur exposition digitale. Nous avons travaillé pour une banque suisse qui était victime d'une tentative de racket. L'opération était

remarquable ; tout était plausible, les courriels étaient parfaits, les structures existaient sur Internet, le nom de domaine était déposé, etc. La sophistication était impressionnante.

Quels conseils auriez-vous à donner à vos camarades polytechniciens en termes de sécurité ?
La sécurité, ou plus exactement la sûreté, est affaire de comportement bien avant l'emploi d'outils. Si ces derniers sont nécessaires pour protéger une structure dans son ensemble, les dirigeants doivent avoir une posture de vigilance. Il faut en particulier s'interroger sur les informations disponibles qui me concernent et qui peuvent être extrêmement utiles pour mener des opérations de *social engineering*. Posture appropriée puis application de procédures assez simples vous permettent de diminuer votre niveau de vulnérabilité de manière non négligeable. Vous diminuez ensuite votre exposition à une cyberattaque par les moyens techniques. Il faut aussi identifier et éliminer le maillon faible face à une attaque, celui-ci pouvant par exemple être un administrateur du SI. Nous avons développé une solution de *war room* qui est complètement indépendante des administrateurs du système *corporate*, parce que couramment, quand il y a une fraude informatique, des administrateurs sont impliqués.


© dimj

"Une stratégie de contre-intelligence économique est la stratégie ultime."

Quelles sont les compétences techniques avec lesquelles vous travaillez actuellement ou dont vous auriez besoin éventuellement ?
Pour les missions de conformité, d'analyse du risque pays et d'exposition au risque digital, nous recrutons essentiellement des profils de type Sciences Po, validés après un stage long. Nous recrutons des informaticiens qui ont une formation du type Epita, Epitech et, la ressource étant réduite, nous formons nous-mêmes des apprentis.
Les jeunes camarades peuvent entrer dans le métier du renseignement en tant que consultants mais notre approche est plutôt de leur conseiller d'acquérir une expérience dans un autre domaine (la banque, l'industrie…) pour bien comprendre le besoin de nos clients. Notre capital, c'est aussi un réseau de correspondants, d'abord dans le monde entier mais aussi parmi les journalistes d'investigation, les recruteurs, les conseils qui sont capables de monter des approches. Une personne en cours de recrutement peut constituer une très bonne source sur ses activités antérieures s'il y a eu un contentieux.
En conclusion, il ne faut pas avoir une attitude paranoïaque (typiquement sur les écoutes téléphoniques) mais il faut comprendre la menace ; à quels types d'attaques suis-je exposé, qui peut les mettre en œuvre, combien cela coûtera-t-il au commanditaire ? Notre expérience sur environ un millier de dossiers traités depuis la création d'Axis nous permet une approche pragmatique, dans l'analyse des signaux faibles d'attaque ou de fraude et dans les actions de protection ou de contre-intelligence à mettre en œuvre, ces dernières devant impérativement relever de la légitime défense. Le terme de « guerre économique » me paraît exagéré mais certaines attaques sont d'une agressivité certaine et menées avec des moyens qui ne sont pas forcément légaux.

Propos recueillis par Alix Verdet

Instruction interministérielle relative à la protection des systèmes d'informations sensibles n° 901 : http://circulaires.legifrance.gouv.fr/pdf/2015/02/cir_39217.pdf

VÉRIFIER MA VULNÉRABILITÉ AU SOCIAL ENGINEERING

Le *social engineering* consiste à manipuler une personne dans le but d'obtenir de sa part des informations normalement secrètes ou confidentielles (un mot de passe, une procédure, le nom d'une personne clef) ou lui faire réaliser une action (un virement bancaire). Les exemples les plus connus de manipulation par *social engineering* sont les fraudes aux présidents, qui, pour faire simple, consistent à contacter une personne clef dans l'entreprise cible (le comptable ou le directeur financier) en se faisant passer pour le président et d'obtenir de sa part un virement sur un compte à l'étranger sous un prétexte crédible. Les données personnelles que nous exposons volontairement ou non servent énormément aux escrocs pour bâtir leurs approches. Le dernier exemple de ce type de fraude a été mis en avant par l'affaire du « faux Le Drian » : les escrocs ont soutiré plus de 50 millions d'euros à leurs victimes en se faisant passer pour Jean-Yves Le Drian alors ministre de la Défense sous François Hollande.

Comment se protéger

1/ La sensibilisation du personnel. Bien que largement médiatisées, ces affaires sont surtout connues des spécialistes de la sécurité.

2/ Vérifier les traces que l'on laisse sur Internet. La notion de protection de la vie privée est largement mise en avant par les politiques ces dernières années (RGPD par exemple) ; or la réalité est que le secret et la confidentialité de la vie privée n'ont jamais été aussi mal protégés. Nos informations personnelles sont partout sur Internet et nous n'en avons pas forcément conscience. Une discipline appelée OSINT pour *Open Source INTelligence* est en train de se développer et de se professionnaliser : il s'agit d'obtenir un maximum d'informations précises sur un sujet ou une cible uniquement en sources ouvertes et donc bien évidemment par le biais d'Internet. Date de naissance, lieu d'habitation, loisirs, membres de la famille, patrimoine. Toutes ces informations peuvent se trouver plus ou moins facilement par recoupement à cause des traces que nous laissons de façon volontaire ou non (réseaux sociaux ; registres officiels…).

Dans les menaces proches du *social engineering* s'est développé sur Internet le *doxxing* ou *doxing*. Il s'agit de collecter des informations à caractère privé dans le but de les diffuser publiquement pour nuire à la personne. De nombreuses personnalités ont déjà fait les frais de ce nouveau sport en voyant leur adresse personnelle ou leur numéro de portable dévoilés publiquement. Plus récemment des personnalités politiques françaises ont fait les frais de ces pratiques.

Aussi pour nos clients nous avons développé une offre « VIP Monitoring » qui consiste justement à évaluer l'étendue des informations personnelles qu'un dirigeant ou un cadre peut exposer sur Internet dans le but de se protéger. Cette offre combine à la fois des techniques de recherche manuelles de l'OSINT mais aussi le développement d'une plateforme logicielle d'investigation permettant l'analyse et la mise en corrélation dans des grandes masses de données disponibles (le fameux *big data*). La logique derrière cet outil est d'agréger des données structurées (par exemple un registre de société), semi-structurées (un *tweet*) ou non structurées (une archive avec des documents PDF, Word, PowerPoint), de les normaliser afin d'extraire des éléments clefs (un e-mail, un numéro de téléphone, un nom, un identifiant unique), de mettre en corrélation toutes ces données mais aussi d'enrichir les résultats à travers des services tiers disponibles sur Internet. Ainsi par exemple à partir d'un simple e-mail il est possible d'identifier un profil LinkedIn, d'obtenir un numéro de téléphone, de trouver les mandats de la personne dans différentes sociétés mais aussi de façon plus anecdotique savoir si notre cible pratique la course à pied et suivre ses parcours quotidiens.

Enfin une analyse de risque est effectuée afin de déterminer comment ces éléments d'informations disponibles en ouvert pourraient être utilisés par un acteur malveillant.

© MJgraphics