Identification et exploitation des failles humaines par les « prédateurs informationnels » : un risque sous-estimé par les entreprises ?

Michel Iwochewitsch

Strateco

Résumé Dans le cadre des tests de pénétration réalisés dans le cadre de la sécurité, peu d'actions développent une approche des "failles humaines". Or, il existe de multiples cas réels ayant démontré la fragilité du "maillon humain" qui peut entraîner des pertes importantes pour les entreprises.

À ce titre, l'intervention porte sur les problématiques de failles humaines – opérationnelles, ou autres – exploitées par les "prédateurs informationnels" afin d'accéder à des informations diverses en fonction de leurs besoins.

La notion de prédateur informationnel regroupe l'ensemble des individus ayant pour objectif de collecter de l'information en provenance de sources humaines pour exploiter celle-ci. À ce titre, au-delà du *social engineer* bien connu (qui pourtant est souvent peu formé), on retrouve également dans cette catégorie, les opérationnels du renseignement industriel, les acteurs de la criminalité organisée, les arnaqueurs, etc.

Malgré des objectifs totalement différents, tous ces prédateurs ont un point commun : ils doivent disposer d'un accès aux informations sensibles de l'entreprise-cible afin d'exploiter ces dernières à leurs profits. **Notre propos est de présenter les principales approches exploitées par ces prédateurs** pour mieux appréhender le risque sous-jacent à ces opérations par essence discrètes. L'auteur rappelle que les techniques/méthodes présentées sont dans la majorité des zones du monde considérées comme illégales et ne sont présentées ici qu'à titre informationnel afin d'illustrer notre propos.

À ce titre, l'auteur rappelle qu'il condamne formellement le recours à ces méthodologies pour accéder à des informations en dehors du cadre spécifique des tests de pénétration informationnelle, réalisés en accord avec l'entreprise cliente et dans un cadre juridique et méthodologique précis.

L'intervention met l'accent sur :
- la compréhension des failles humaines et son exploitation ;
- l'identification des failles telle que réalisée par les prédateurs
- les méthodologies déployées par ces prédateurs pour collecter de l'information sensible.

Compte tenu de la sous-estimation régulière du risque que représente ces prédateurs informationnels, le premier objectif de l'intervention est de comprendre le mode de fonctionnement de ces derniers afin de pouvoir reproduire lors des tests de sécurité informationnelle les méthodologies de collecte, afin de mieux cerner les failles de son entreprise.

Le second objectif est de permettre d'appréhender le risque que représentent ces menaces dans le dispositif de sécurité mis en place par la société, afin de pouvoir mettre en place des mesures efficaces d'identification et de minimisation de ces risques.

Les failles humaines dans le domaine informationnel... Un vaste sujet qui nécessiterait plusieurs ouvrages pour en faire le tour ! Nous ne ferons donc qu'effleurer ces approches dans le cadre de ce document.

Avant d'aborder le cœur du sujet, nous tenons à préciser que si ces outils peuvent être exploités éthiquement et en toute légalité dans le cadre strict d'un test de pénétration, *la majorité des approches retenues par les prédateurs, sont quant à elles parfaitement illégales.*

Rappelons que la directive européenne 95/46/CE sur la vie privée, interdit ce type d'approche (profils de personnalité par exemple) sur un ressortissant européen sans son acceptation formelle pour le recueil des informations privées nécessaires. De plus, dans de nombreuses législations européennes, la collecte d'informations confidentielles – y compris sous forme orale – est condamnable (cas en France d'une information classifiée). ***Ces approches ne sont présentées ici que dans un cadre pédagogique : l'auteur rappelle qu'il condamne fermement le recours à des approches illégales !***

Regroupée généralement sous le vocable Social engineering dans le monde informatique, l'exploitation des "failles humaines" rassemble toute une famille de techniques s'appuyant sur la même "cible" : le cerveau ! Parler de failles humaines n'est-ce pas un peu présomptueux ? Il serait en effet plus juste de parler de failles du système d'exploitation de notre cerveau.

Appréhender les failles du cerveau réveillant de nombreux tabous liés essentiellement à notre vision d'une forte stabilité de notre personnalité, il nous semble important de souligner deux points :

1. Le cerveau – cette merveilleuse "machine à penser" – intègre des failles, des erreurs de perception, et des schémas cognitifs (*cogwebs* en terme plus intime) plus ou moins fiables. *Shocking* ! Le plus bel instrument que la terre n'ait jamais porté pourrait contenir des erreurs ? Impossible ! Et pourtant. *Des biais cognitifs aux erreurs de perception, en passant par les heuristiques, les scientifiques ont documenté au cours de la dernière décennie les nombreuses failles de notre cerveau !*
2. Malgré les progrès réalisés au cours des vingt dernières années, quant à notre compréhension tant des personnalités que du cerveau humain, *il n'existe pas à notre connaissance – fort heureusement – de possibilité de classer les humains dans des "petites cases" formatées !*

Mais comment donc ces prédateurs – qui exploitent sans vergogne nos pauvres têtes – agissent-ils ? En pratique, des failles identiques sont exploitées avec des objectifs distincts par toute une série de cousins de la grande famille des "prédateurs informationnels" :

Le social engineer (SE) qui généralement manipule ponctuellement un individu pour contourner des dispositifs de sécurité et/ou obtenir une information considérée comme confidentielle ;

L'officier traitant œeuvrant dans le renseignement offensif qui cherche à disposer d'une source humaine sur le long terme, ainsi que son pendant dans le monde privé, le spécialiste du renseignement industriel ;

Le spécialiste du perception management[1] qui s'appuiera sur les failles d'un individu pour induire en erreur ce dernier afin de limiter sa capacité décisionnelle ;

Le désinformateur dont l'objectif avoué est de tromper, et dont l'efficacité est décuplée par l'exploitation de ces failles ;

L'opérationnel en guerre de l'information (infowar) et le spécialiste des *psyops* qui exploiteront ces failles pour entraîner des dysfonctionnements dans les moyens de communication de son adversaire par exemple et/ou obtenir diverses actions (allant de l'adhésion, au refus de combattre) d'un groupe d'individus ;

Les arnaqueurs en tout genre ainsi que les groupes transnationaux de criminalité organisée comme par exemple les spécialistes du *phishing*. Dont les attaques sont facilitées par l'exploitation de ces failles.

Si évidemment l'existence même de ces failles est un bonheur sans fin pour tous ces vilains personnages, rappelons qu'il s'agit d'un véritable cauchemar en termes de sécurité !

Malgré de multiples différences applicatives, le point commun entre tous ces "cousins prédateurs" reste l'exploitation des failles humaines ! Comment font-ils pour les identifier ? Les exploiter ? Sur la base de quelles approches ? Ces questions sont fondamentales dans l'approche de ces prédateurs mais également, lors des tests de pénétrations informationnels.

Comme le dit un vieux proverbe, *un bon garde-chasse est avant tout un excellent braconnier* ! De fait, mettre en place des procédures limitant l'impact de ces failles, revient peu ou prou à développer une méthodologie proche de celles exploitées par les prédateurs dans leur travail quotidien.

Rappelons ici le principal intérêt de ces méthodes dans le cadre de votre entreprise : étalonner le degré de perméabilité de votre entreprise aux approches de SE[2] et de renseignement.

1 L'identification des failles par les prédateurs

1.1 Les catégories de failles

Quatre catégories ont été retenues dans notre approche professionnelle (cf. figure 1) :

Les failles opérationnelles : par failles opérationnelles, nous entendons toutes les failles découlant des activités régulières de l'entreprise. Il en existe évidemment des dizaines, mais les plus fréquentes sont : la prédictibilité des opérations ; les procédures et la mise en œuvre opérationnelle de ces dernières ; les faibles procédures en cas "d'incident" informationnels ; les "traces extérieures "(voyages, cartes de crédits, factures de téléphones) ; l'outsourcing et la multiplication des sites ; la gestion des contractants ; la "fragilité intrinsèque" de certaines directions (marketing, public relation, commercial, RH) ; la recherche d'efficience qui entraîne – par regroupement des acteurs – des fragilités en cas de pénétration ; une organisation de la sécurité basée sur la préconception erronée de "l'attaquant extérieur", etc.

Les failles humaines : Nous ne pourrons dans le cadre de cet article intégrer l'ensemble des failles humaines exploitables. Pour approfondir le sujet, nous renvoyons en notre lecteur sur différents sites de références[3]. Néanmoins, les failles humaines les plus universelles concernent : la personnalité ; les biais cognitifs/heuristiques ainsi que les grandes lois d'influence ; et les failles "classiques" répertoriées par les services de renseignement (un exemple, MICE : Money, Ideology, Compromission, Ego). À ces failles universelles se rajoutent des failles plus personnelles comme les "phases de déstabilisation" telles qu'un divorce, un décès, des problèmes financiers, etc. On intègre également dans cette catégorie les failles environnementales ayant un impact direct sur "le moral des troupes" et qui cristallisent les failles précédentes comme le harcèlement et les plans sociaux, qui facilitent l'exploitation des autres failles humaines ! D'autres failles naturelles sont souvent présentes dans les entreprises : l'absence de *chinese wall*, les services administratifs ; les "radio lavabos" ; l' "îlot RH" qui par ses prérogatives "bloquent" des informations importantes.

Les failles physiques : très nombreuses, ces dernières regroupent les failles découlant d'une situation physique ! Parmi les plus fréquentes, on trouve : l'absence ou le faible contrôle des points d'entrée (ex : typique le parking extérieur permettant d'étudier les véhicules des employés pour détecter par exemple des individus ayant des soucis financiers, et/ou dépensiers) ; une localisation

[2] SE : *Social Engineering*

[3] www.healthbolt.net/2007/02/14/26-reasons-what-you-think-is-right-is-wrong/

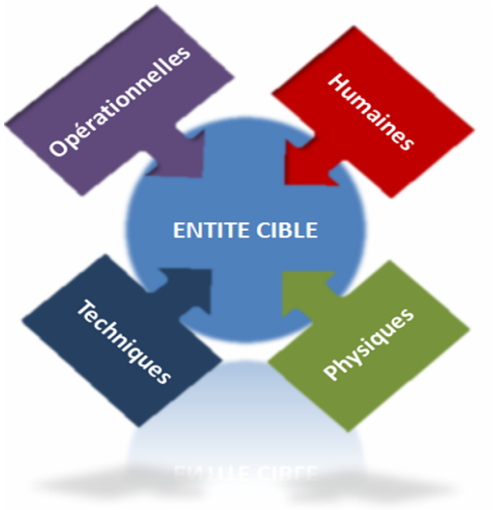

FIG. 1: Les catégories de failles retenues

physique facilitant les opérations techniques ; le gardiennage de faible qualité (formation/motivation) ; le voisinage dans les *open space* ; les serrures fragiles et/ou sous-exploités ; les bureaux mal rangés ; les stocks extérieurs de matériels ; le stockage électronique outsourcé (ex :archives confiées à une société extérieure) ; le *waste archeology* (fouille des poubelles) des déchets (rappelons que même shreddés les documents peuvent être reconstitués si le shreddage ne respecte pas certaines normes de qualité) ; les bureaux mal rangés ; l'absence de procédure (ou son non respect) de sécurité des PC (passwords, écran de veille, etc.) ; les points fragiles naturels (ex : le copieur/imprimante et son disque dur) ; et la portabilité des équipements électroniques actuels (depuis l'apparition de ces outils, le volume de documents "volés" est en nette augmentation ! Un seul exemple : le cas célèbre Ericsson où l'opérateur a emporté "l'équivalent papier" d'une dizaine de 33t sur des CD-ROM), etc.

Les failles techniques : par technique nous entendons l'ensemble des failles pouvant être exploitées par un mode technique. Ces derniers allant de la pénétration informatique – que nos lecteurs connaissent beaucoup mieux que nous – à la sonorisation[4] d'un lieu, en passant par la surveillance électronique, le Tempest, les EMP, etc. Les principales familles de failles dans cette catégorie sont : les failles logicielles, erreurs de configuration, des outils informatiques ; la gestion des passwords ; le stockage des archives ; les canaux de transmission (interne/externe) de l'information ; les réseaux et points d'accès déployés ; les EMP[5] et approches Tempest[6] dont les coûts de fabrication ont fortement diminué ces dernières années ; les techniques de sonorisation des lignes (fax/voix),

[4] Mise sous surveillance par microphone

[5] Selon des rumeurs fréquentes ces dernières années, des sociétés de la City ont fait l'objet de chantage à l'EMP exploitée pour détruire les supports physiques des transactions financières de la journée

[6] Un "bon" document sur le phénomène Tempest : http ://www.cl.cam.ac.uk/techreports/ UCAM-CL-TR-577.pdf

des lieux qui vont de l'ultrasophistiqué réservé aux services officiels, à des outils simples à prendre en main et suffisant pour de nombreux cas de renseignement industriel.

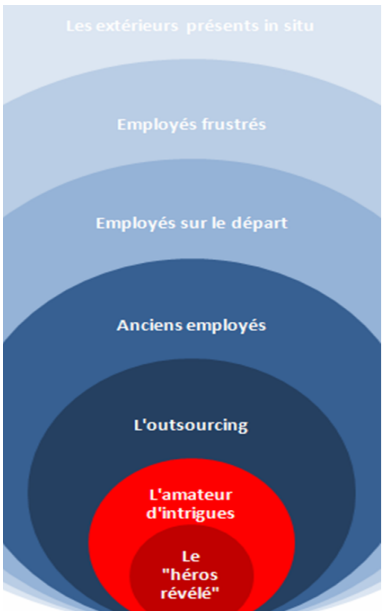

FIG. 2: Les grandes catégories d'internes exploitables dans l'entité (classé selon la dangerosité risque/capacité de contrôle sécuritaire)

Un rappel : les failles sont évidemment combinatoires chacune pouvant s'appuyer sur les autres pour être plus efficaces ! Ainsi, on considère que le cœur est généralement la famille de failles opérationnelles, que les failles humaines renforcent toutes les autres, que les failles techniques et physiques facilitent les accès aux autres failles...

1.2 L'identification d'individus précis

Le prédateur s'attache ensuite à identifier des individus susceptibles de pouvoir être "exploités". En général, **les opérationnels disposent de leur propre grille d'analyse qui reprend les différentes catégories d'individus les plus intéressants**. Quelques exemples : les "invisibles" ayant accès aux informations sensibles (employé du centre de reprographie, femmes de ménages, assistantes, etc.), cadres en charges de projets sensibles, comptables, direction commerciale, etc. **Ces catégories standards sont ensuite analysées en fonction d'une grille des profils stéréotypés les plus fragiles** (cf. figure 2). Sont recherchés à ce stade : la frustration individuelle ou d'un groupe, les anciens employés (si possible en conflit ouvert ou larvés), les employés sur le départ (avec analyse des motivations : rappelons que ces employés ont encore leurs accès et qu'ils peuvent être "fragilisés"), évidemment les "extérieurs" présents in situ (sociétés de services de secrétariat, d'accueil, femmes de ménages, maintenance informatique, sécurité, etc.). **Le**

prédateur s'attachera à identifier des individus pour chacune de ces catégories. Cette étape franchie, une analyse plus fine des failles humaines est initiée pour sélectionner les individus les plus fragiles. Toutes les grilles d'analyse sont alors déployées : fragilités basiques (MICE), émotionnelles, stéréotypes de profils à risques (cf. figure 3), psychologique et de personnalités, fragilités médicales, etc.

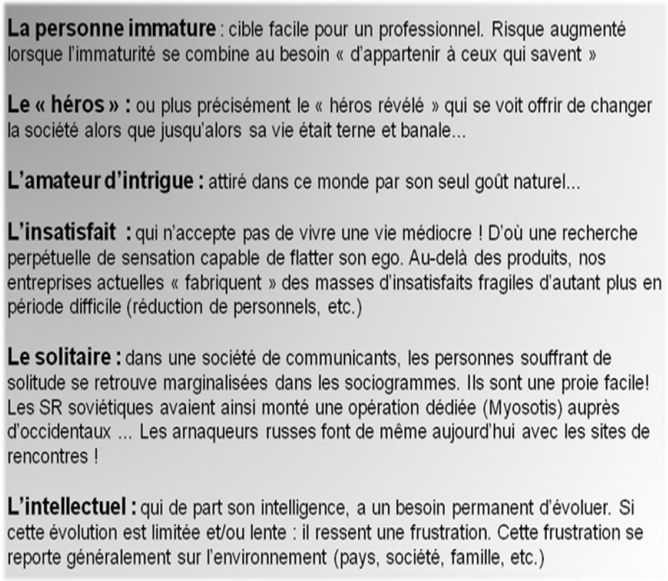

FIG. 3: Quelques stéréotypes d'individus "à risque" recherchés par les professionnels pour leurs fragilités

Cette analyse s'appuie cette fois-ci sur une surveillance approfondie et ciblée[7] sur les individus sélectionnés ! Fondamentalement, l'objectif du prédateur est de mettre autant de moyens techniques, humains, financiers que possible sur cette phase qui "assure" la réussite des recrutements ultérieurs ! L'objectif est "de savoir ce qu'il faut savoir "pour manipuler l'individu lors du recrutement. En particulier ce que l'individu ne veut pas que les autres sachent de lui...

L'Agent Acquisition Process (figure 4) Pour illustrer les étapes d'un recrutement d'un individu – qui va au-delà du traditionnel SE – nous utiliserons la terminologie en vigueur dans les services spécialisés US nommé l'Agent Acquisition Process, ou l'Asset Acquisition Process.

Ce process comprend 7 phases distinctes. Les couleurs correspondent à une représentation graphique des risques inhérents pour le prédateur.

- Vert = peur de risque d'être découvert ;
- Rouge brique = risque d'identification des opérateurs nécessitant la mise en place de procédure d'OPSEC spécifique ;

[7] Pouvant inclure sans être limitatif, le *waste archeology*, la surveillance physique, la sonorisation des lieux de vie, le piratage des PC privés, l'approche d'individus dans divers réseaux de la source, etc.

– Rouge vif = phases au cours desquelles le risque est le plus élevé pour l'opérateur.

Avant d'aborder le *process* a proprement parler, il convient de noter que derrière chacune des phases, l'opérateur dispose d'un ensemble de méthode lui permettant de réaliser son recrutement dans les meilleures conditions. Ces méthodes vont au-delà du cadre de ce document et d'ailleurs, ne sont pas utiles pour mettre en place une défense efficace.

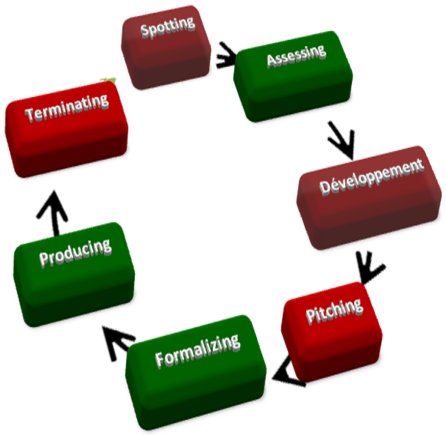

FIG. 4: L'Agent Acquisition Process

Décomposons maintenant nos 7 phases :

1. **Spotting** : cette phase reprend la partie d'identification d'un individu précis. Généralement, elle fait l'objet d'approches discrètes du sujet (élicitation par exemple) pour valider l'intérêt de la source potentielle au-delà de ses fonctions "prometteuses".
2. **Assessing** : phase plus ou moins longue (de quelques semaines à quelques mois en environnement protégé), les objectifs sont simples : connaître l'individu, le profiler[8], identifier les failles les plus exploitables et les moins dangereuses pour l'opérateur. Rappelons que le process est discret : la source ne devant pas se rendre compte de cette phase, ou des suivantes jusqu'au pitch.
3. **Development** : la phase de développement de la source est complexe, délicate et potentiellement dangereuse pour l'opérateur. L'objectif est de "faire partie" de l'environnement de la source, puis de développer une relation – de plus en plus intime – avec cette dernière. En clair : "devenir le nouvel meilleur ami" de sa source ! Selon le réseau initial retenu (professionnel, privé, etc.), et les approches sélectionnées, cette phase est plus ou moins longue. C'est également lors de cette phase que *l'assesing* est poursuivi cette fois-ci pour valider les failles identifiées. Ainsi, le traitant peut proposer dans une escalade parfaitement maîtrisée – nommée désensibilisation – à la source de "s'investir" de plus en plus dans la relation tout en testant ses failles. Le traitant offrira dans le même temps des "excuses" à sa source afin d'alimenter la rationalisation de

[8] Confère l'article de l'auteur dans MISC 34

cette dernière[9]. Une fois amené à un point précis permettant le *pitch*, l'opérateur pourra soit réaliser ce *pitch* seul, soit "transférer" la source au *pitcher*. L'intérêt de transférer le contact est de renforcer les OPSEC en cas de problèmes futurs et également de ne pas remettre en cause directement la relation source/prédateur1 en cas d'échec du *pitch*.

4. **Pitching** : une fois "mûre", les opérationnels proposent à la source un pitch ! En clair, il s'agit d'une offre claire de recrutement. évidemment, si l'offre est "claire", la présentation de cette dernière peut faire l'objet de prétextes particuliers. C'est ici que les résultats des phases précédentes trouvent tous leurs sens... Plus la source est "connue", plus il est possible de "customiser" l'offre. Le prédateur utilisera tous les moyens possibles pour faciliter ce passage. Comme le soulignait Victor Ostrovsky dans son ouvrage le plus connu : *"The idea of recruitment is like rolling a rock down a hill... You take somebody and get him gradually to do something illegal or immoral. You push him down the hill. We didn't blackmail people. We didn't have to. We manipulated them"*.
5. **Formalizing et Producing** : il s'agit ici des phases les plus simples pour l'opérateur. La première consiste à fixer le cadre de la collaboration et la rémunération. La seconde de mettre en place les transmissions de besoins et le retour d'informations. évidemment, l'opérateur continue d'évaluer en permanence la source – mais aussi les informations transmises. Il offre également des "moyens de résoudre" la dissonance cognitive permanente ou ponctuelle de la source. Pourquoi former des sources ? Pour assurer les OPSEC de l'opération premièrement[10], et assurer une meilleure productivité en terme de collecte tout en les "protégeant" le plus possible pour éviter leur identification. Enfin, une formation même succincte aux méthodologies du renseignement donne l'illusion aux sources d'être "dans le secret", et calme les plus anxieux.
6. **Terminating** : toute bonne chose ayant une fin, il arrivera à un certain stade que la source devienne inutile. Plusieurs raisons expliquent cet état de fait : la source peut être mutée et n'a plus d'accès intéressants, le projet est terminé, elle est donc inutile, sa qualité est médiocre, etc. Dans tous les cas de figure, la situation est dangereuse pour l'opérateur ! En effet, la source "lâchée" peut ressentir de l'animosité, un manque (relation privilégiée), une envie de se dénoncer au service de sécurité, un manque financier (la source de revenus se tarissant), etc. Dans tous les cas de figure, cette phase nécessite un talent certain de l'opérateur pour "terminer" la relation dans les meilleures conditions de sécurité ! Dans le monde du renseignement industriel, cette phase peut être accompagnée d'un bonus, et aller jusqu'à l'exposé de mesures de rétorsions envers la source qui voudrait se dénoncer...

2 L'exploitation des failles humaines

2.1 La boîte à outils du parfait petit prédateur informationnel

Le métier de prédateur est somme toute simple. Son dilemme ? Faire parler – et/ou faire agir – des inconnus pour qu'ils commettent des erreurs de jugement suffisantes afin qu'il puisse accéder à des informations sensibles.

En clair, toutes les opérations montées par un prédateur, reposent sur deux éléments pivots :

[9] Phénomène de dissonance cognitive décrit dans l'article MSIC sur le *profiling*.

[10] À ce titre, les sources seront également formées aux méthodes sécurisées de transmission des informations physiques (BLM, lieu physique de dépôt des documents en "boîte lettre morte" avec un système de signalisation et une protection) ou électroniques selon des procédures rigoureuses protégeant les opérateurs

1. collecter de l'information sensible ;
2. obtenir des documents.

Ici, nous désirons introduire un bémol quant à l'utilisation de ces outils. En effet, à l'inverse d'un système d'exploitation, où les logiciels ont des fonctionnalités précises, il est essentiel de retenir qu'en aucun cas ces outils ne permettent de mettre les humains dans "des petites cases" ! L'auteur s'oppose à cette simplification, courante dans certains milieux.

Cependant, et grâce entre autres à une fiabilité croissante, ces outils permettent d'améliorer l'efficacité d'un prédateur grâce à la systématisation de processus d'influence largement documentés par des travaux "de terrain" [11].

De la notion de *rapport* Rapport ? En terme technique, il s'agit d'un état entre deux individus permettant d'optimiser le flux de communication ! En clair : le prédateur va exploiter des outils pour devenir le "meilleur nouvel ami" de ses cibles en un temps record. La place manque dans ce document pour aborder en profondeur l'ensemble des techniques disponibles, et ce point fera l'objet de différents slides lors de la présentation. A minima pour renforcer le rapport, le prédateur cherche avant tout à :

- exprimer de l'empathie pour la situation de sa cible (par ex. en insistant sur les difficultés du métier, en offrant une oreille compatissante, etc.) ;
- donner l'illusion à la cible qu'il partage de nombreux points communs avec lui ;
- donner l'illusion à la cible qu'il peut "changer" les choses pour elle, soit en supprimant un désavantage, soit en offrant des avantages (argent, sorties, expertise, etc.).

Afin de faciliter ce travail de rapport, le prédateur doit pouvoir s'adapter à sa source. C'est à ce titre qu'il va exploiter différents outils de *profiling* pour mieux connaître son interlocuteur

Le profil de personnalité (*profiling*) Terme barbare s'il en est ! Le *profiling* consiste peu ou prou à définir les principales caractéristiques d'un individu. Il s'agit d'un sujet éminemment complexe qui ne peut-être détaillé en quelques lignes. Cependant, deux points doivent être présents à l'esprit lorsque l'on parle de profil de personnalité. Le premier est que *les instruments développés au cours de la dernière décennie sont considérés par les professionnels comme pertinents et d'une grande fiabilité.* À titre d'exemple, une approche comme celles des *Big Five* (OCEAN par ex.) est ainsi créditée d'une fiabilité de 0.9 et, est considérée universelle (quelque soit la culture ou l'origine ethnique de l'individu).

D'autre part, ces outils permettent d'identifier les principaux traits structurels d'une personnalité, et non l'intégralité de la personnalité d'un individu ! Pour prendre une métaphore, vous pouvez utiliser de multiples manières des œufs, du sucre, de la farine, et du lait (les traits structurels) pour réaliser de nombreuses pâtisseries différentes (la personnalité). Les ingrédients (traits) sont stables et présents dans chaque gâteau (personnalité), et pourtant le résultat est différent entre un cookie et un quatre-quarts !

Deux familles d'outils sont plus particulièrement utiles pour le prédateur :

Le OCEAN : outil de profil considéré comme le plus pertinent disponible à ce jour. Techniquement, les outils dérivant du OCEAN (tels le NEO-PI-R[12] ou l'IPIP[13] que vous pouvez tester en

[11] À ce titre, l'ouvrage de référence reste le "Perloff" : The Dynamics of Persuasion, ISBN 0805840885

[12] Une courte présentation du NEO-PI-R : http ://www.ecpa.fr/uploaded/newsletter/ fiche-tec2003_neopi.pdf

[13] Le site de référence de l'IPIP : http ://ipip.ori.org/

ligne) permettent de classer chaque individu en fonction de 5 traits de personnalité considérés comme structurants et répartis selon un axe allant de 0 à 100 :

O : Openness to experience évaluant le degré d'ouverture d'un individu aux expériences nouvelles allant de Preserver (O–) à Explorer (O++)

C : Conscientiousness allant du Flexible (C–) spontané et confortable dans le "multi-tâches" au Focused (C++)

E : Extraversion évaluant le degré d'extraversion d'un individu d'Introvert (E–) à Extravert (E++)

A : Agreeableness évaluant le degré d'adaptabilité aux autres d'un individu allant du Challenger (A–) au Adapter (A++)

N : Neuroticism qui évalue le degré de réaction au stress allant d'un Resilient (peu sensible N–) au Reactive(de type anxieux N++)

L'EDS : l'Executive Decision Making Style[14] il s'agit d'un outil d'analyse permettant d'étudier deux éléments essentiels de la prise de décision :

– l'analyse d'une situation au travers de l'utilisation des informations disponibles (Information Use) ;
– la formulation d'une décision au travers du degré de focalisation (Focus).

L'EDS permet donc de déterminer les caractéristiques de la prise de décision en fonction de l'exploitation de l'information disponible (allant de la décision immédiate avec peu d'informations, à l'individu désirant exploiter le maximum d'informations avant de décider) et le nombre d'alternatives que définira l'individu (axe allant de la mono-décision au recours à différentes alternatives). Pour d'évidentes raisons d'efficacité, connaitre le mode habituel de décision d'une cible est essentiel pour le prédateur ! Ce dernier peut en effet mieux contrôler la présentation de ses effets s'il sait comment la cible a l'habitude de réagir...

2.2 Faire parler ... Ou l'art de l'élicitation

Encore un mot barbare ! *Quid* de l'élicitation ? Il s'agit tout simplement d'une méthode de collecte s'appuyant sur des techniques psychologiques optimisant le ratio discrétion/efficacité. Schématiquement, l'opérateur définit en fonction du profil de la cible, les méthodes les plus efficaces.

Les principales méthodes peuvent être regroupées en catégorie comme précisé dans la figure 5.

Prenons un exemple concret, si la cible du prédateur est un extraverti (E+ ou E++ en OCEAN), ce dernier opterait pour la gestion du silence comme technique principale. La raison ? L'extraverti déteste plus que tout, les ruptures dans le flux de communication ! Or, le silence – comme d'ailleurs les questions – sont considérés comme des ruptures de flux. Le prédateur prendra donc l'habitude d'exploiter volontairement le silence pour "pousser" un extraverti à révéler plus d'informations que nécessaire.

Plusieurs techniques d'utilisation du silence peuvent ainsi être exploitées. Avec un extraverti, tentez l'expérience suivante en maintenant un silence de 5 à 10s après :

– Une réponse de la source... Pour obtenir plus de détails...
– Une phrase de la source... Pour relancer le sujet...
– Une question du collecteur... Pour "forcer" la réponse de la source...

Généralement, le choix des techniques d'élicitation (on en dénombre environ une centaine à ce jour) repose sur une analyse du contexte dans lequel interviendra l'opérateur. Plusieurs modèles d'analyses cohabitent.

FIG. 5: Les principales techniques d'élicitation

Pourquoi ne pas simplement utiliser l'approche traditionnelle de l'interview en exploitant un jeu de questions ? Plusieurs raisons à cela ! La principale – fondamentale – est qu'un individu se souviendra toujours des questions posées au cours d'un entretien et des réponses apportées ! Comme précisé en infra, les questions sont des "marqueurs de ruptures de communication" ! Rappelons que le prédateur a tout intérêt à laisser la cible dans l'ignorance de son action. En résumé, le mantra du prédateur pourrait être "pour vivre heureux, vivons caché" ! Un bon prédateur cherche donc en permanence à laisser ses cibles dans une approche heuristique[15] pour éviter une trop forte cognition (cf. figure 6 sur l'ELM).

2.3 Persuader

Vaste sujet que celui-ci ! Comment est-il possible de persuader un interlocuteur de remettre des informations à un parfait inconnu devenu récemment un "nouvel meilleur ami" ? La littérature scientifique à ce sujet est fournie, nous nous permettrons donc de renvoyer nos lecteurs intéressés aux références pour y trouver des informations complémentaires.

[15] http ://changingminds.org/ explanations/theories/ heuristic-systematic_persuasion.htm

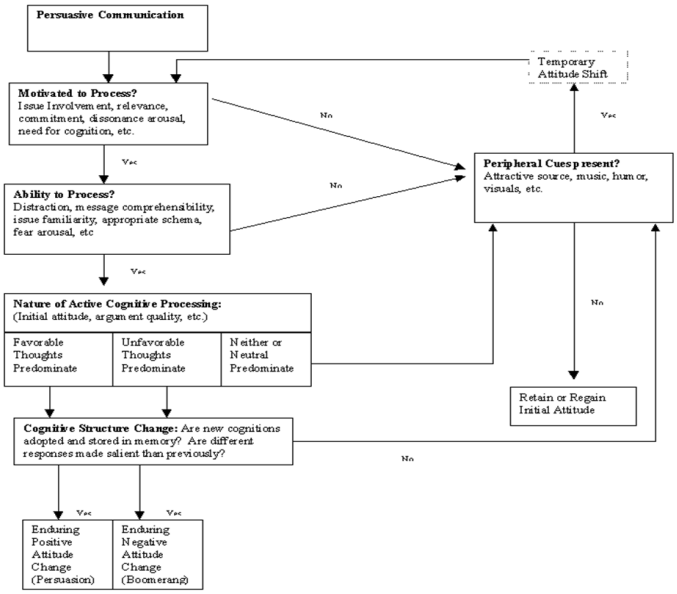

FIG. 6: L'Elaboration Likelihood Model : défini en 1980 par Cacioppo et Petty, l'ELM est considéré comme un des modèles de persuasion les plus pertinents dans les milieux spécialisés. La théorie de l'ELM s'appuie sur l'existence de deux "routes" de persuasion. La voie centrale s'appuie sur la motivation initiale du "persuadé" et ses possibilités d'actions cognitives. Cette voie nécessite de prendre en compte de nombreux paramètres comme l'attitude initiale de la cible, etc. La voie périphérique se développe quant à elle lorsque le "persuadé" ne peut pas/ne veut pas développer de processus cognitifs (ce qui correspond peu ou prou au mode heuristique).Dans ce cas de figure, l'opérateur exploitera surtout des variations de formes du message (en faisant appel à toute la gamme de biais cognitifs et heuristiques) pour obtenir l'adhésion de la cible. De fait, chaque voie nécessite des approches de persuasion différente : le contenu est fondamental en voie centrale, et la forme en voie périphérique.

Néanmoins, il existe de nombreuses techniques s'appuyant sur une connaissance de plus en plus approfondie du cerveau. Des experts comme Cialdini[16], Cacioppo (cf. l'encadré n°3 sur l'ELM), Joule & Beauvois[17], ou Guéguen[18], ont vulgarisé au cours des dernières années de nombreuses techniques exploitables.

Globalement, il est possible de classer ces techniques / méthodes en trois catégories :

[16] Le site web de Cialdini (http ://www.influenceatwork.com/), une page reprenant ses principaux travaux : (http ://en.wikipedia.org/wiki/Robert_Cialdini), et son ouvrage de référence : Influence, ISBN 0688128165

[17] Petit traité de manipulation à l'usage des honnêtes gens, ISBN 2706102918

[18] Psychologie de la manipulation et de la soumission, ISBN 2100055046

1. Les méthodologies ayant permis de faire émerger un modèle d'exploitation : l'exemple type est l'Elaboration Likelihood Model[19] de Cacioppo qui permet d'exploiter au mieux les schémas heuristiques (cf. encadré n°6) ;
2. Les "grandes lois d'influence" qui se déclinent en diverses techniques. Ainsi par exemple, le principe du contraste qui peut techniquement se "traduire" dans la technique de la "porte au nez" (cf. grands principes d'influence) ;
3. Les "boutons" présents dans le cerveau et qui comprennent les principaux biais cognitifs et heuristiques (cf. cf. grands principes d'influence).

D'un point de vue opérationnel, on exploite ces catégories en débutant par la définition d'un ELM de la cible/situation. Puis, en fonction du profil, on sélectionne les lois d'influences. Ensuite, on exploite les biais et heuristiques pour, soit renforcer les approches sélectionnées, soit "perturber" les capacités de jugement de la cible pour mieux passer sous son radar.

Quelques grands principes d'influence

L'autorité : célèbre depuis l'expérience de Milgram... le principe d'autorité reste à ce jour l'un des plus simples à mettre en œuvre ! Prenons un exemple : quand avez-vous la dernière fois remis en cause le jugement de votre médecin lorsqu'il vous a prescrit un médicament ?

Le recadrage ou framing : fondé entre autres approches sur les travaux de Kahneman et Tversky, , il s'agit d'une des techniques les plus versatiles ! Ses variantes sont multiples (positifs ou négatifs, de positionnement, par contraste, par attribution, etc.) En effet, il apparaît que la forme du message (*framing*) permet d'obtenir plus facilement l'adhésion d'un individu.

La dissonance cognitive : théorisée en 1957 (Festinger), cette loi repose sur un principe simple : les individus agissent de façon conforme à leurs valeurs/croyances et sont mal à l'aise lorsqu'ils sont en dissonance. En cas de dissonance, les individus adaptent leurs comportements futurs pour les supprimer ! Différentes approches de réduction de la dissonance sont utilisés : refus/-rationalisation/séparation/modification du cadre de référence.

Réciprocité et obligation sociale : comme le dit un proverbe japonais : "rien n'est plus coûteux que quelque chose donné gratuitement..." ! La théorie s'appuie sur le principe de réciprocité entraînant un besoin de retourner la faveur... C'est la loi la plus simple à mobiliser ! Les grandes approches sont : l'échange de secrets/ les concessions réciproques/ les "cadeaux" en phase initiale.

L'usage du contraste : fondé entre autres éléments sur les réactions quasi-automatiques de l'archicortex, cette loi est simple à mettre en œuvre ! La technique la plus connue s'appuyant sur ce principe est "la porte au nez". Sans rentrer dans le détail de cette dernière, il s'agit grosso modo de commencer par exposer l'individu à une requête trop "coûteuse" (argent, temps, implication, etc.) afin d'obtenir un refus. Puis dans un second temps d'exposer la véritable requête. Le premier refus permettant généralement d'obtenir satisfaction sur la seconde requête qui parait tout à la fois plus raisonnable en terme de "coût" (logique du contraste) et qui permet à l'individu qui a refusé quasiment par réflexe la première requête de proposer une alternative (contraste appliqué à la dissonance cognitive).

Quelques biais cognitifs et heuristiques

[19] http ://www.tcw.utwente.nl/theorieenoverzicht/Theory clusters/Health Communication/ Elaboration_Likelihood_Model.doc/

L'effet de primauté : nous retenons plus aisément une 1ère information que celles qui suivront (rôle de l'archicortex)

L'effet de halo : consiste à étendre à l'intégralité d'un ensemble un jugement – positif ou négatif – qui aura été porté à son encontre à partir d'un seul élément.

Le biais de connaissance rétrospectif : consiste à projeter de nouvelles connaissances dans le passé et à se les réapproprier. Ce biais est à l'origine d'une auto manipulation de la mémoire.

Le biais de complaisance égocentrique : nous avons une fâcheuse tendance à nous approprier nos réussites et à refuser nos échecs. En limitant notre capacité d'analyse sur les causes de nos échecs et de nos réussites, ce biais nous "aide" à réaliser de mauvaises analyses.

l'heuristique de disponibilité qui nous pousse à estimer une fréquence ou une probabilité en fonction de la facilité avec laquelle des exemples et/ou des associations nous viennent à l'esprit. Ainsi, lorsque nous avons un jugement à faire, ce dernier se fera en tenant compte des informations les plus facilement accessibles.

3 Se protéger

Voici succinctement présentées les principales failles humaines exploitables par les prédateurs. Une question de fond demeure : est-il possible de se protéger contre de telles actions par définition discrète ? Notre réponse est clairement un OUI !

Néanmoins, nous considérons que se protéger contre ces actions par essence discrètes est délicat, voir difficile ! Pour prendre un parallèle avec la gestion des systèmes d'exploitation, combien de failles dans les systèmes d'informations sont "ouvertes" par un humain...

Considérez ensuite que ces erreurs humaines reposent peu ou prou sur une palette très large de failles que le prédateur informationnel a appris à identifier, puis à exploiter !

Multipliez ensuite ces failles par le nombre d'individus dans votre société...

Selon notre propre expérience, mettre en place une protection "anti-failles humaines" est possible. Elle doit débuter par un "test d'intrusion" pour marquer les esprits ! Ce test doit aboutir à une présentation des résultats (sous une forme anonyme) aux employés. Les "révélations" du test sont un excellent moyen de limiter la déperdition d'informations liée à une simple formation[20]. La séance initiale doit ensuite s'accompagner d'un programme intégrant à minima :

des formations régulières de sensibilisation ;

des procédures d'alertes qui doivent à minima comprendre une hotline permettant de reporter les appels "étranges". évidemment, la ligne en elle-même n'a aucun intérêt si elle n'est pas accompagnée d'une procédure permettant d'étalonner la dangerosité potentielle. Cette procédure devant couvrir l'ensemble des "prédateurs informationnels" sous peine d'être inopérante ! Pour prendre un parallèle dans la vie privée, il serait idiot de protéger ses enfants contre les seuls risques de "prédateurs sexuels" ("ne monte pas dans la voiture d'un inconnu", etc.) alors que la majorité des cas de violences de ce type sont liés à des individus évoluant dans un environnement familier ;

des procédures de protection de l'information idéalement gérées par un cadre de l'entreprise – qui ne doivent pas se limiter à une classification de l'information (par essence impossible à

[20] Rappelons à ce titre que certaines études ont démontré que 90% du "message" était perdu par l'absence de processus de mise en œvre suite à une formation

maintenir dans le contexte actuel) mais proposer une approche globale permettant aux employés d'acquérir une sensibilité à l'information. Compte tenu du coût élevé d'une telle approche, nous intégrons une analyse approfondie des informations à protéger (intégrant les contraintes risques et temps) pour établir une typologie, avant de définir d'un système de protection (pouvant intégrer un *cloaking*[21] par ex.) ;

des procédures de gestion similaires à celles adoptées dans les cellules de crise – pour circonvenir les risques détectés.

Si la pertinence de ces "tests d'intrusions humains" est évidente au vu des enjeux, la difficulté de mise en œuvre d'une telle procédure rend malheureusement complexe des tests grandeur nature. En effet, pour qu'un test d'intrusion humain soit efficace, il doit à minima :

- Et contrairement aux tests d'intrusion informatique, *ne pas être limité dans les méthodes déployées pour le mener à bien* (la seule limitation étant évidemment d'entraîner un employé dans un acte illégal, comme l'amener à accepter une rémunération).
- Plus particulièrement, ce test ne doit pas se limiter à obtenir des accès aux réseaux informatiques. *Il s'agit d'un test d'intrusion reposant sur les failles humaines : son objectif est donc très clairement d'accéder par tous les moyens disponibles aux informations sensibles de l'entreprise.*
- *Reposer sur une éthique forte !* En particulier concernant la confidentialité des informations collectées et la protection des sources (qui dans ce cas de figure sont des employés et dont l'anonymat doit être préservé y compris vis-à-vis de son employeur).

4 Conclusion

Si le format de ce document reste extrêmement simplifié, il n'en reste pas moins que ces procédés sont actuellement utilisés par l'ensemble des prédateurs informationnels lorsqu'ils jettent leurs dévolus sur une cible ! évidemment, pour assurer une parfaite discrétion à ces approches, il faudrait plusieurs mois pour enchaîner la phase initiale d'identification à l'analyse de la pleine "production" des sources humaines. Rappelons un axiome de tous les métiers collectant de l'information : "l'information est au centre des process de l'entreprise" ! Nous rajouterons que sans informations fiables, aucun prédateur n'est capable dans sa spécialité de "toucher" sa cible ! Qu'il s'agisse de collecte, de désinformer, de perturber, de voler, ou encore d'arnaquer.

Le renseignement est la fondation sur laquelle le prédateur s'appuie pour monter ses opérations ! Et dans ce cadre, l'identification des failles et des individus est LE *process* essentiel qui détermine l'efficience de toutes les actions ultérieures...

L'auteur rappelle par ailleurs, qu'il condamne fermement le recours à ces approches offensives – souvent illégales – sauf dans le cadre fixé contractuellement et légalement, d'un test de pénétration informationnelle. *D'ailleurs – y compris dans ce cas- , il est illégal et d'ailleurs non-éthique de monter de vraies opérations de recrutement d'employés !*

[21] Dérivée du monde aéronautique (avion furtif), le *cloaking* est une approche permettant de présenter à l'extérieur de multiples "facettes" d'un projet sensible afin d'embrouiller les capacités de collecte d'un concurrent

Il est cependant obligé de convenir que les *Spooke*[22] ne sont pas rares dans les événements professionnels comme les salons... Ce qui souligne probablement une forme de demande plus ou moins discrète.

Par ailleurs, pour "briser le cou" à un vieux fantôme : dans le contexte actuel, toute entreprise peut devenir la cible pour de multiples raisons de ce type de prédateurs ! La concurrence exacerbée (renseignement industriel par ex.), la simple existence de "l'entreprise cible" (cas de la criminalité organisée par ex.), peuvent être suffisantes pour devenir une cible.

Plus évidemment, des opérateurs du renseignement industriel sont impliqués, plus la cible a peu de chance de détecter les actions compte tenu du degré de professionnalisme de ces acteurs. Mais rappelons quand même qu'un simple arnaqueur avec des méthodes basiques, est capable de vous coûter très cher en temps et en argent !

Fort heureusement, en comprenant les modes opératoires des prédateurs informationnels, il est possible de mettre en place des procédures de protection.

La tâche est néanmoins complexe ! Compte tenu des avancées phénoménales dans la compréhension des failles du cerveau, vous comprendrez les difficultés qui vous attendent pour limiter ces dernières face à un groupe d'individus déterminés...

D'ailleurs, vous-même, ne vous arrive-t-il jamais de parler d'un sujet que vous ne devriez pas aborder sur un *tchat* ? Ou entre amis un soir devant une bonne bouteille de vin...

Gardez à l'esprit que l'exploitation volontaire et professionnelle *d'une seule faille d'un cerveau d'un individu "placé au bon endroit"*, peut rendre caduc des années de labeur et de R&D, en contournant des dispositifs – informatiques ou autres – de plusieurs centaines de milliers d'euros !

[22] Un des "petits noms" des experts privés du renseignement industriel