Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2018)
Heft: [2]: Numéro Thématique 2

Artikel: La somme de toutes les peurs, variante 2018 : crises qui dérapent et téléphones-espions
Autor: Chrzanovski, Laurent
DOI: https://doi.org/10.5169/seals-823459

Cyber

La somme de toutes les peurs, variante 2018 : Crises qui dérapent et téléphones-espions

Laurent Chrzanovski
Rédacteur en chef, *Cyber Security Trends*

Pour les amateurs de cinéma, l'adaptation aux écrans du roman de Tom Clancy, la *somme de toutes les peurs* (1991) reste une référence. Tourné en 2002 sous la houlette de Phil Robinson, le film met en scène Ben Affleck, dans le rôle de Jack Ryan – le «mythique» analyste de la CIA de la série de Clancy –, parvenant à lui seul à éviter au dernier moment une 3e Guerre Mondiale entre les Etats-Unis et la Russie. On y observe, à la perfection, comment un ennemi intérieur largement assisté par une stratégie obsolète, le manque de confiance, des décisions inadéquates et de mauvais renseignements peuvent conduire à une catastrophe si une crise majeure parvient à toucher le cœur du système.

Plusieurs forces armées disposent désormais d'unités spécialisées dans les actions cybernétiques.

Si nous avons fait référence à la crise imaginée par Clancy, c'est parce que nous avons vécu deux événements historiques qui auraient pu dégénérer de façon dramatique. Il s'agit d'abord de la seconde tentative de coup d'Etat de Moscou, celle de 1993. Si nous sommes restés enfermé chez nous les 2 et 3 octobre, lorsque les échanges de tirs nourris, entre troupes d'élite et snipers paramilitaires, ont causé près de 2000 morts parmi les civils des groupes antagonistes réunis autour du parlement et de la tour de télévision d'Ostankino, le lundi 4 au matin, à savoir le jour même de l'assaut final du Parlement, nous avons pu aller travailler au Musée d'Histoire, sis sur la Place Rouge! Notre paternel remplissant alors les fonctions de Chargé d'Affaires à l'Ambassade de Suisse, nous étions logé dans un appartement de l'un des immenses immeubles construits par l'URSS pour les diplomates occidentaux, à deux pas de l'un des points les plus stratégiques de la capitale, la Place des Trois Gares. Sur quelques centaines de mètres carrés, on y trouve à la fois les trois gares ferroviaires les plus fréquentées de Moscou (Yaroslawski, Kazanski et Leningradski), et l'une des stations de métro les plus utilisées de la capitale, «Komsomolskaya». Dans une période où l'insécurité quotidienne et l'impuissance politique étaient au maximum, nous sommes restés sans mots en découvrant un système de sécurité aussi impressionnant que parfaitement huilé. Outre de nombreux snipers placés sur les toits des gares, des tanks et des blindés légers appartenant respectivement aux divisions d'élite Kantemirovskaya et Tamanskaya régnaient sur la place. Les accès aux gares et au métro étaient constitués de plusieurs points de contrôle consécutifs, gérés par des *miliciens* (policiers) ordinaires, révolvers dans l'étui, placés sous les ordres stricts des soldats des unités d›élite de *spetsnaz*, *in primis* Alpha et Vympel. Les check-points étaient fluides, le calme serein affiché par soldats aidait grandement à calmer la nervosité palpable des policiers, tandis que les rames circulaient, comme toujours, toutes les 50 secondes. A aucun moment, tout comme lors du premier coup (1991), un scénario «à la Clancy» n'aurait été possible. La verticale du pouvoir (de l'armée et des

«services») était assurée et leur loyauté aux deux présidents acquise, et ce malgré l'extrême impopularité de ces dirigeants au sein de ces mêmes institutions.

Le second moment tragique auquel nous avons assisté s'est déroulé le 9 novembre 2005. Nous étions à Amman pour y codiriger un congrès et y avons ouï les déflagrations des trois attentats-suicide d'Al Qaeda. Après un jour de couvre-feu, le surlendemain, nous avons pu conduire hors de la capitale, passant chaque 5 km. les points de contrôle de l'armée. Là aussi, des militaires au calme olympien et, à chaque bloc, un seul soldat, placé en second plan, avait le doigt sur la gâchette.

Ces deux événements démontrent à la perfection que si le centre névralgique d'un système de sécurité (ici celui de deux Etats) est humainement préparé à affronter le pire, c'est à dire l'ennemi intérieur (le cas russe) ou le terrorisme (le cas jordanien), la panique ou la nervosité n'ont pas leur place, donc aucune chance de chaos.

Cette parenthèse «non digitale» était nécessaire à mettre en lumière deux enjeux sécuritaires principaux auxquels se confrontent les entreprises mais aussi, dans le cas de la Suisse, l´armée.

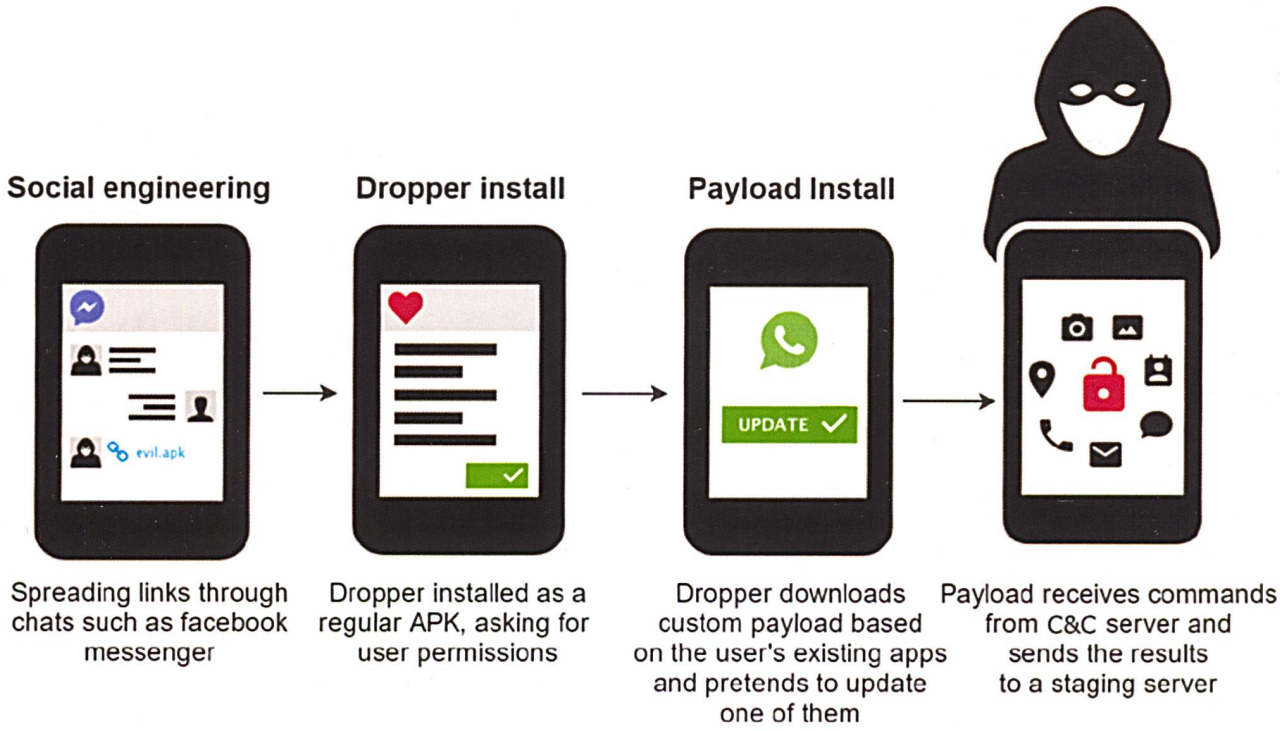
Ces deux défis relèvent purement de la sphère comportementale. Le premier se base sur l'analyse de deux des secteurs les plus résilients «*by design*», puisqu'une attaque peut entraîner des conséquences tragiques voire des pertes humaines : le domaine du transport aérien et celui des infrastructures énergétiques. Les entreprises qui y consacrent leurs activités sont particulièrement bien dotées en moyens humains et techniques pour faire face à un panorama de dangers aussi permanents que mutants – on a abandonné le terme de persistants – et à des groupes organisés dont la polyvalence et l'expertise technologique s'améliore quotidiennement. Elles mènent régulièrement des exercices de crise, mais la désuétude des modèles utilisés commence à être sérieusement mise en question.

Pour ces deux secteurs, l'entreprise BeST a réalisé des «*war-games*» en temps réel, entre autres le désormais célèbre «Scenario», réalisé sur commande de la IATA et couvrant les besoins des multiples silos qui constituent l'écosystème sécuritaire, technique, humain et logistique du transport aérien. Dans une conférence récente, Dotan Sagi, fondateur de l'entreprise et principal animateur de ces immersions en crise réelle, a fait part d'un constat alarmant. Lors des exercices qu'il mène régulièrement y compris pour le compte de la cellule cyber-sécurité du premier-ministre israélien, ce ne sont jamais les gouvernants, les militaires, les services de renseignement ou les forces de l'ordre qui posent problème. Le problème principal est constitué par les luttes intestines au sein d'une même entreprise, fruit de rancœurs personnelles entre collaborateurs, de mésentente entre les départements, de peur de la direction ou, à l'inverse, d'abus de pouvoir de celle-ci.
Le résultat? Dans plusieurs entreprises de ces deux secteurs vitaux, les cellules de crise étendues en viennent

à oublier tout sens du devoir et des responsabilités, aggravant la crise et communiquant de façon chaotique et parfois même contradictoire, voire refusant de communiquer avec d'autres entreprises concernées par la même attaque... *la somme de toutes les peurs*. Selon les propres sondages menés par BeST – dans le pays doté de la plus enracinée des mentalités de défense et de sécurité au monde – près de 75% des employés des sociétés sondées n'ont aucune confiance dans leurs collègues de travail. Or, si ces phénomènes ont été observés dans des secteurs – auxquels on peut ajouter la finance et le luxe – où la culture de sécurité est l'une des clés de voûte du business, on s'imagine bien dans quel état errent les entreprises des autres secteurs de notre économie.

Sociologiquement, dans le cadre d'une armée de milice comme la nôtre, il faudra tenir compte de ce facteur. La «génération Facebook» est aujourd'hui adulte et, pour ces jeunes très individualistes, les amis sont ceux qui ont les mêmes goûts et les mêmes idées. Cette donnée doit être associée au fait qu'il n'y a et de loin ni esprit d'équipe ni fierté des employés d'appartenir à une «communauté», contrairement aux propagandes que l'on peut lire dans les prospectus édités par les entreprises. Le collègue est un concurrent, les départements tiers sont des étrangers, le chef direct est le chef réel – le CEO étant sur une autre planète – et la concurrence, loin d'être à abattre, a peut-être un meilleur job à offrir. Dans le cas d'une crise réelle et majeure, il faudra donc faire preuve de talents hors-pair de leadership pour faire travailler tous ces conscrits à l'unisson, quel que soit leur grade, dans une obligation de collaboration vouée à un résultat rapide et constructif.

Le second défi est un corollaire du précédent, la «*génération Facebook*» étant aussi la «*génération smartphone*». Il s'agit donc d'urgence d'anticiper les effets du passage au 5G, multipliant par 30 la vitesse des données accessibles avec les smartphones et autres tablettes. L'association des deux maillons les plus faibles de la chaîne cyber-sécuritaire, l'humain et le smartphone, est un défi majeur puisque depuis deux ans, plus de la moitié des données sont accédées grâce à cet outil «*insecure by design*», et qu'en 2020, ce seront plus de 85% des données que les utilisateurs consulteront par ce moyen et non plus par un PC.



Les étapes de l'attaque cyber via un téléphone portable.

Ce n'est pas un hasard si c'est bien dans ce domaine que deux des meilleures armées au monde viennent de faire face aux plus inattendus des dangers.

Le cas le plus récent est celui qui a vu le Pentagone s'opposer à *Strava*,[1] l'application gratuite pour smartphones destinée au joggeurs et aux cyclistes. Pour ce faire, elle utilise un serveur gratuit de cartographie, permettant à tout sportif de se mesurer à d'autres sur un même parcours. Quand la US Army a refusé de répondre à la question du nombre de soldats tués ou blessés à cause de cette application, tout en ne niant pas fermement d'avoir subi des pertes, l'affaire a rempli les pages des journaux de spécialité. En effet, tout un chacun, terroristes compris, pouvait accéder aux itinéraires des joggeurs du Pentagone ou de sites classés secret défense, comme les périmètres de la base aérienne avancée de Sarrine, au Nord-Est de la Syrie, ou celui de l'énorme base de l'OTAN à Kandahar en Afghanistan: on y voit parfaitement les parcours des soldats-joggeurs à l'intérieur et à l'extérieur des bases (jaune: parcours les plus fréquents).

Plus intéressant pour la Suisse, la mésaventure subie par l'armée israélienne montre en revanche la vulnérabilité des recrues, comme l'a magistralement démontré Ido Naor,[2] spécialiste au sein du Global Research and Analysis Team de Kaspersky. En 2016, le hasard a fait que plusieurs jeunes recrues ont eu des problèmes techniques avec leur smartphone, demandant conseil à des spécialistes de l'armée. L'alarme a aussitôt sonné au C4I de l'IDF, qui a chargé son *Information Security Department* et mandaté Ido Naor comme spécialiste externe du cyber-crime.

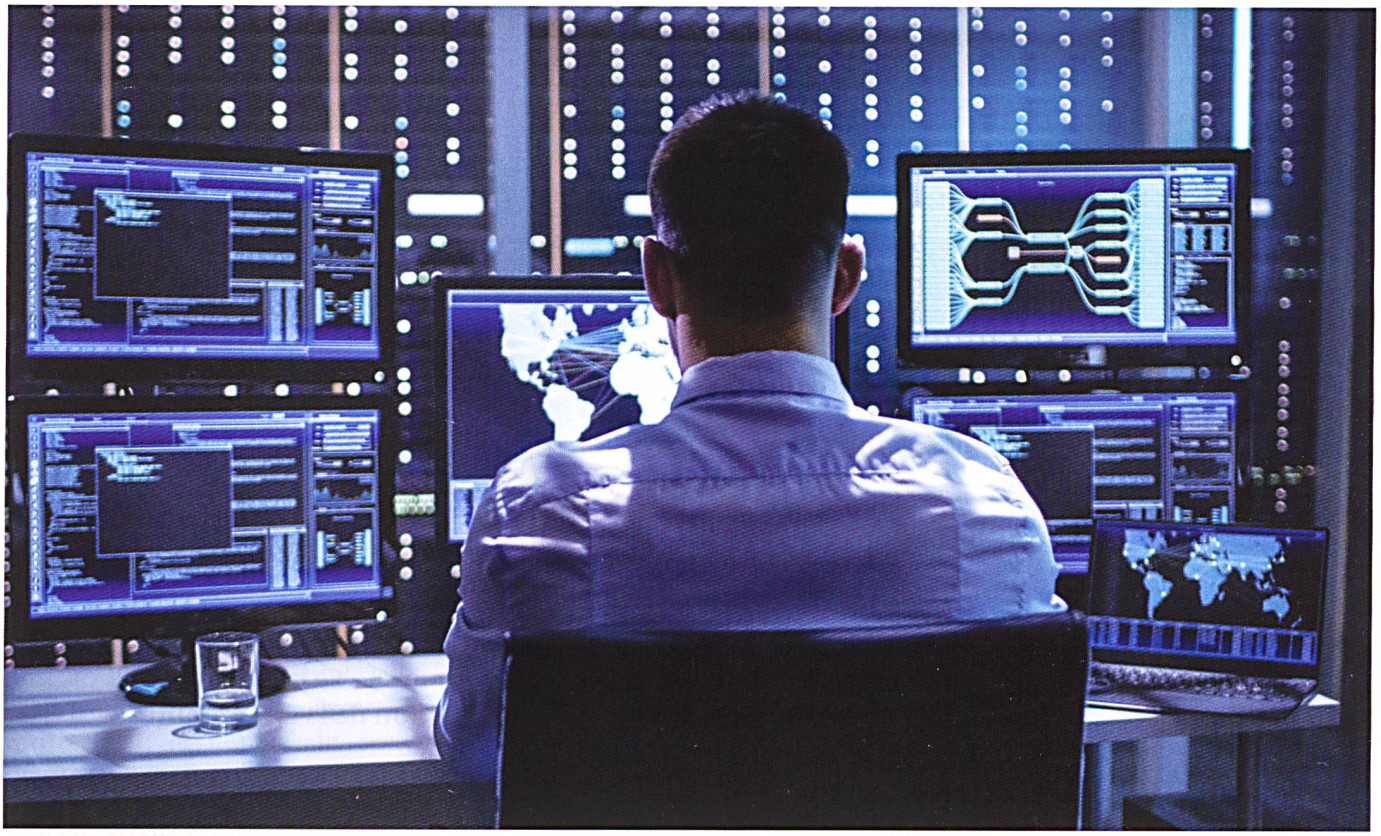
Et pour cause : durant des mois, un groupe criminel avait dressé de faux profils séduisants dans le but d'infiltrer les recrues de l'IDF et, grâce à un «paquet d'applications», de pouvoir utiliser leur smartphone à son bon vouloir, micro et caméras compris. Ce traquenard, conçu selon l'adage «*plus c'est gros et plus ça passe*» se basait sur la création de faux profils Facebook de nombreuses – et jolies – jeunes filles juives canadiennes, du même âge que les recrues, cherchant des «amis» pour leur prochain séjour de six mois en Israël. Dans une seconde étape, seules les recrues ayant répondu et mentionné qu'elles sont stationnées près de la bande de Gaza ont mérité l'attention de ces demoiselles, qui ont par la suite incité leurs «amis» à télécharger plusieurs applications afin de pouvoir se parler, échanger, partager de la musique. C'est l'une de ces applications, recelant un puissant spyware mais mal ficelée, qui a posé des problèmes à certains portables, dévoilant le pot aux roses.

Le système utilisé pour infiltrer les recrues ©Ido Naor et Kaspersky Labs

La traque à l'auteur réel a duré peu de temps, grâce aux talents des chercheurs, à la polyvalence de l´équipe et aux nombreuses traces laissées par les hackers: les analyses

1 Cf. N. Sotira, Quand le sport peut devenir un problème de sécurité nationale, Cyberseurity Trends France 2018/1, pp. 52-3 (https://issuu.com/cybersecuritytrends/docs/ct_2018_no1_fr)

2 I. Naor, Breaking The Weakest Link Of The Strongest Chain, in Securelist (16.02.2017): https://securelist.com/breaking-the-weakest-link-of-the-strongest-chain/77562/



Il est d'autant plus difficile de se protéger contre des attaques cyber que celles-ci peuvent survenir simultanément et en grand nombre.

de l'hébreu utilisé dans les faux comptes, le décryptage des codes de programmation, les adresses IP utilisées pour envoyer et recevoir des données, tout cela a permis de localiser les auteurs, qui opéraient depuis une base du Hamas au sein même de la Bande de Gaza. Dans la plus préparée des armées au monde, plus d'une centaine de soldats avaient été victimes d'un piège aussi simple qu'efficace, heureusement décelé à temps grâce à la négligence de ses auteurs !

Nul doute que les stratégies et les mesures à prendre en ce qui concerne les cadres d'utilisation des smartphones des conscrits, mais aussi des officiers, vont devoir être drastiquement revues, de même que le nombre de salles militaires munies de parois anti-5G ou de brouilleurs anti-G. Plus que jamais, «*spy*» devrait remplacer «*smart*» dans le préfixe que l'on donne à nos portables, si vulnérables qu'ils sont bien plus facilement au service d'un ennemi qu'à notre «disposition».

L. C.

Les installations nucléaires iraniennes ont été ciblées par plusieurs attaques dont les effets n'ont été visibles qu'au bout de plusieurs années (Stuxnet).