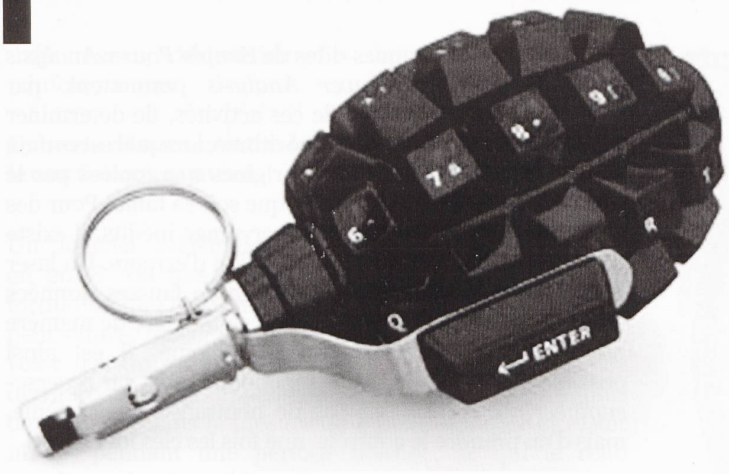
Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2014)
Heft: 6

Artikel: La cyberdéfense, nouveau front de guerre
Autor: Weck, Hervé de
DOI: https://doi.org/10.5169/seals-781189



En 2013, les Nations Unies ont déterminé qu'une cyber attaque n'était pas un acte de guerre. Ceci permet donc à ceux qui s'en servent de se faufiler sous le seuil de la guerre et risque de ne pas être, dès lors, soumis au droit des gens en temps de guerre.

Renseignement

La cyberdéfense, nouveau front de guerre (1e partie)

Col Hervé de Weck

Ancien rédacteur en chef, RMS

Les Etats, les entreprises, les privés également multiplient les parades contre les cyberattaques qui visent ordinateurs, serveurs, tablettes et téléphones portables. Quasiment tous les gouvernements en arrivent à penser que leurs homologues, proches ou lointains, mènent contre eux des offensives cybernétiques, alors qu'en même temps ils doivent faire face à des actions de hackers (*pirates*) groupés ou solitaires. Le cyberespace, voilà le nouveau champ de bataille qui s'ajoute à l'espace terrestre, maritime, aérien et spatial. Il n'est soumis à aucune loi, et les attaques qui s'y déroulent ne laissent en général pas de traces, ce qui empêche des ripostes efficaces. Internet favorise l'anonymat, les falsifications d'identité, l'utilisation d'ordinateurs et de serveurs sans que les propriétaires s'en aperçoivent.

On prétend qu'un opération sophistiquée, donc dangereuse et difficile à contrer, ne peut provenir que d'organes d'Etats développés ou de forces armées modernes et bien équipées, mais pas d'individus en sandales portant des *kalachnikov*... Les guérillas, les djihadistes ont pourtant intégré une dimension technologique à leurs actions, ainsi la techno-guérilla pratiquée par le Hezbollah libanais.

Une attaque informatique est une agression comme une autre; les services de renseignement et de sécurité ont tout avantage à développer des capacités en cyberdéfense, afin de détecter des indices d'attaques, même sur la base d'indices infimes. Une attaque catastrophique peut se produire contre des infrastructures vitales propres à un pays, comme la distribution d'eau ou les transports. Il semble même que de multiples petites *piqûres d'abeilles* provoquent des conséquences plus déstabilisantes au niveau national qu'une grande attaque.[1]

Le ministre français de la Défense, Jean-Yves Le Drian, déclare en janvier 2014: « La France doit se préparer à une guerre cybernétique. *(...) C'est une de mes priorités, car nous faisons face à un accroissement des risques, qu'il s'agisse de paralysie des systèmes étatiques ou d'attaques visant à détruire nos moyens d'information ou de commandement. (...) En 2013, nous avons répertorié 780 incidents significatifs au sein du ministère de la Défense[2], contre 195 en 2011. (...) Ce sont en général des attaques de faible ampleur, provenant d'une puissance étrangère ou d'un groupe d'activistes (...).* »[3]

Les cyberattaques ont doublé depuis 2010

En 2012, la police et la gendarmerie françaises enregistrent 1427 atteintes à des systèmes de traitement automatisé de données, contre 626 en 2010. Dans 20-30% des cas, elles ont altéré, modifié ou supprimé des données. Ces chiffres n'éclairent que la pointe émergée de l'iceberg, car ils recouvrent uniquement les cas les plus sérieux qui ont justifié une plainte. Les entreprises, les privés ne le font pas systématiquement, question d'image de marque, de honte ou de volonté de ne pas révéler des activités problématiques.

Les éditions Economica à Paris proposent une collection de cyberstratégie

Aymeric Bonnemaison; Stéphane Dossé: *Attention: Cyber! Vers le combat cyber-électronique*. Préface du général d'armée Bertrand Ract Madoux, chef d'Etat-major de l'armée de terre. Postface du contre-amiral Arnaud Coustillière, officier général à la cyberdéfense. Paris, Economica, 2013. Commencé en 2012, le texte est achevé en été 2013.

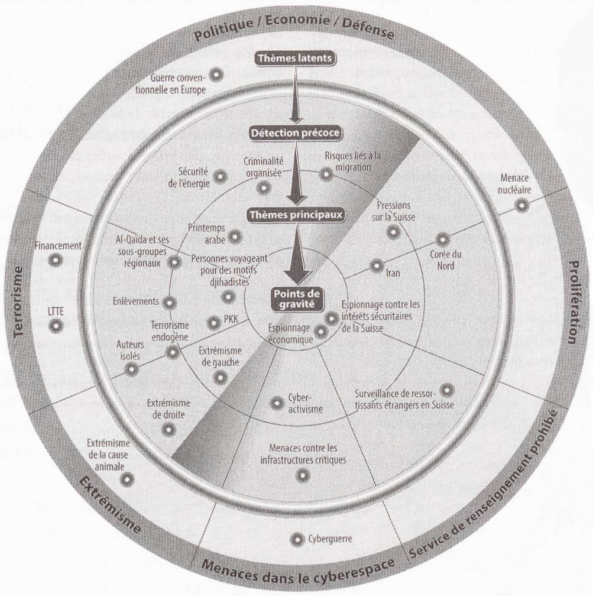
Quelques aspects techniques

Les hackers qui déclenchent une attaque en Suisse peuvent se trouver en Chine, dans les pays de l'Est, en Afrique, aux Etats-Unis ou... dans le Gros-de-Vaud; ils

1 *Le Point.fr* – publié le 29 janvier 2014.

2 5% auraient été vraiment compliquées à résorber.

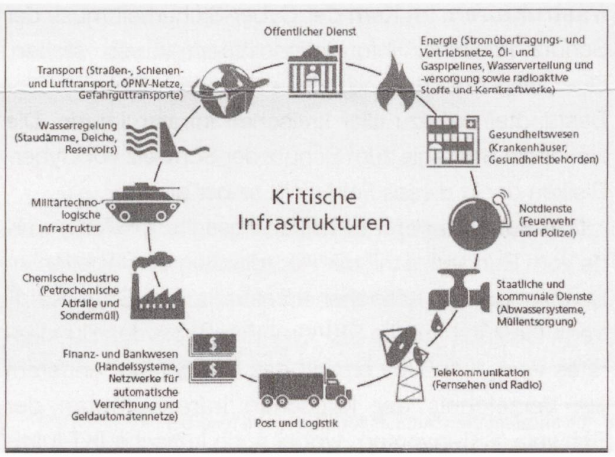
3 *Les Echos*, 21 janvier 2014.



fonctionnent en réseaux, se retrouvent sur des forums dédiés. Certains agissent pour le compte d'Etats, même démocratiques. Souvent, on ne peut les localiser et les identifier, car leurs ordinateurs, leurs serveurs ne portent pas d'IP, de plaque d'immatriculation.

Plutôt que de décrypter les données d'un système de communication très protégé, de manière aléatoire par la méthode dite de *Brute Force Cracking*, par l'entremise de dictionnaires ou de bases de données baptisées *Rainbow Table*, on s'en prend directement au calculateur chargé de chiffrer les informations, afin d'en intercepter les clés. Comme un cambrioleur qui utilise un stéthoscope, afin de déterminer l'usure des parties du mécanisme de fermeture du coffre-fort, plutôt que de l'ouvrir en essayant toutes les combinaisons possibles, il est possible, grâce à des instruments de mesure en vente libre, de *monitorer* l'activité électrique et magnétique des circuits électroniques d'un calculateur opérant un algorithme de cryptage.

On surveille l'activité des circuits de l'un des systèmes au moment de l'échange des clés destinées à chiffrer leurs



interactions. Les attaques dites de *Simple Power Analysis* ou de *Differential Fower Analysis* permettent, par l'interprétation statistique de ces activités, de déterminer les traitements réalisés par l'algorithme, lorsqu'il est connu, et d'en déduire les données d'origines manipulées par le système, donc la clé, cela quelle que soit sa taille! Pour des matériels ou des algorithmes de cryptage inédits, il existe des méthodes de *Fuzzing* par injection d'erreurs. Un laser ou un courant électrique *bombarde* de fausses données certaine s parties d'un circuit par, ce qui altère de manière mesurable le comportement du système. Il est ainsi possible d'en reconstruire le fonctionnement par *reverse-engineering*. Il ne s'agit pas de neutraliser un système, mais d'en prendre le contrôle, une fois les clés identifiées.

Une contre-mesure efficace consiste à faire réaliser par le logiciel de cryptage des opérations inutiles mais fortement consommatrices en courant électrique, afin de perturber le travail des hackers. En raison du nombre de systèmes d'armes qui communiquent entre eux, produits avant l'identification de ce type d'attaque et de la rareté de l'expertise au sein des Etats, l'utilisation de cette technique reste encore très limitée.

Pour éviter de dévoiler, sans le vouloir, des informations stratégiques comme l'emplacement d'une unité combattante ou des activités en cours, il convient de désactiver le système de géolocalisation sur Facebook, de s'abstenir de filmer pendant un engagement. Depuis 2013, une application bloque les principales fonctions – caméra, micro, internet – des smartphones lorsqu'ils se trouvent dans l'enceinte d'un site sensible. Aucun système ne peut cependant éliminer tous les risques, car l'individu reste le maillon faible de n'importe quel système de sécurité.

On ne saurait, bien entendu, oublier les moyens de protection classiques de données hyper-sensibles, comme la mise en place de réseaux particuliers, non reliés à internet, l'utilisation d'ordinateurs hors de tout réseau, la conservation non électronique mais physique (archives-papier). Le problème est de définir quelles données doivent faire l'objet de tels traitements.

Les six étapes d'une cyberattaque

1. *Ciblage.*- Découverte d'un site ou d' un serveur intéressants, envoi d'un *malware* pour les infiltrer.
2. *Exploitation de la vulnérabilité.*- Recherche des failles de la machine, du serveur et du réseau, compréhension du fonctionnement de la cible.
3. *Reconnaissance technique.*- Le *pirate* obtient les droits d'administrateur qui lui permettent d'agir directement et de manière plus discrète.
4. *Déploiement.*- Vérification de la méthode utilisé, préparation d'un écran de fumée pour camoufler l'intention de l'attaque.
5. *Lancement de l'attaque.*- Récupération des informations sensibles, transmissions sur des serveurs *amis*. Plus simple à effectuer, la destruction est préconisée plutôt que l'exfiltration.
6. *Sabotage.*- L'opération terminée, éventuel sabotage

du réseau, destruction des données ou de l'outil informatique.

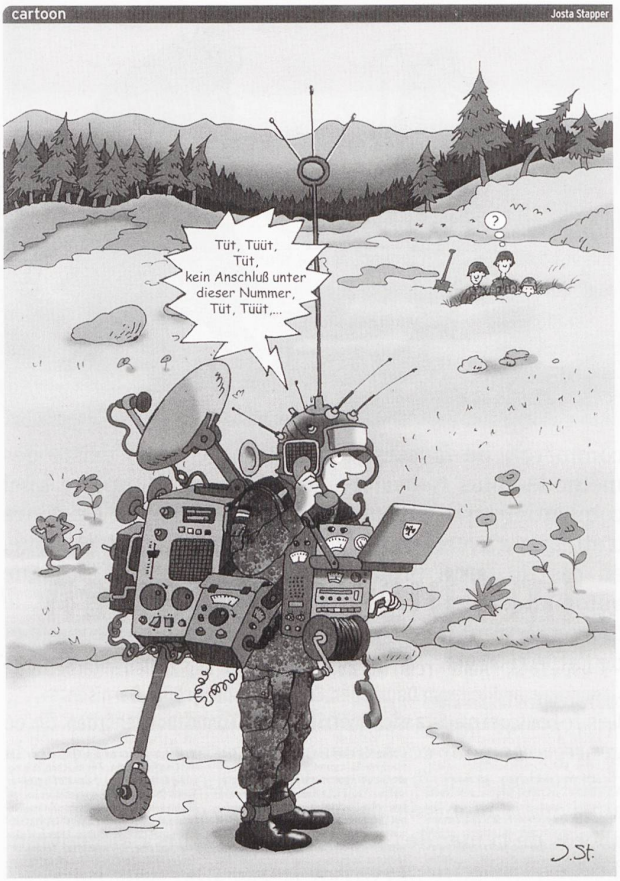
Cybermenaces contre les Etats et leurs forces armées

Un logiciel malveillant, baptisé *agent.btz*, introduit en 2008, via une clé USB, dans un ordinateur d'une formation de l'Army américaine basée au Proche-Orient, peut saturer un serveur, détruire des données et, surtout, voler des informations grâce à une *porte dérobée*. Sa dernière version, appelée *Snake*, s'avère encore plus dangereuse, dans la mesure où il peut *hiberner* et rester inactif pendant une période donnée, ce qui le rend quasiment indétectable.

Selon le BAE Systems Applied Intelligence, appartenant à un groupe britannique spécialiste dans la cybersécurité, 56 cas d'infection ont été constatés depuis 2010, dont 44 depuis 2013. L'Ukraine semble particulièrement visée avec 32 cas, dont 22 depuis la fin 2013, ce qui coïncide avec la crise politique qui a abouti à la destitution du président pro-russe Ianoukovitch[4]. Des développeurs hautement qualifiés, appartenant vraisemblablement à un service de renseignement russe, semblent se trouver derrière cette cyberattaque.

Pendant presque quatre ans jusqu'en octobre 2014, une opération de cyberespionnage menée depuis Téhéran sur les réseaux sociaux (Facebook, Twitter, LinkedIn, Google+, Youtube, Blogger) permet d'espionner au moins deux mille personnes, notamment des diplomates et des militaires américains, dont un amiral quatre étoiles. Les hackers, usurpant l'identité de journalistes, de fonctionnaires et de collaborateurs de la Défense, contactent leur cible. Un site d'information fictif, newsonair.org alimenté par des reprises dans les médias, renforce leur crédibilité. La liaison établie, ils envoient à leurs victimes des liens les invitant à se connecter sur des pages factices, afin de récupérer leurs identifiants et leurs mots de passe. Les renseignements collectés peuvent servir à développer des systèmes d'armes, à connaître l'opinion au sein des forces armées américaines, l'état de l'alliance américano-israélienne, à prendre l'avantage dans des négociations entre Washington et Téhéran.

Déjà en 2012, des Chinois usurpent sur Facebook l'identité de l'amiral américain James Stavridis, commandant de l'OTAN en Europe, ce qui leur permet d'obtenir des comptes privés mail, des photos, des messages et des réseaux des amis de l'amiral... Le ministre français de la Défense, le chef d'Etat-major de l'armée de terre sont aussi les cibles de telles opérations. Depuis le lancement de l'opération SERVAL au Mali, beaucoup de cyber-attaques visant la France proviennent du sud de la Tunisie. En 2010, des sites de régiments français engagés en Afghanistan[5], destinés à informer les familles, sont infiltrés à des fins subversives et pour faire des repérages sur certaines familles.



Un hacker turc à la fin 2013, dans le but déclaré de dénoncer la conservation de mails au-delà des délais légaux, en rend public près de 77'000 stockés par la branche islandaise de Vodafone. Son action met en lumière la faiblesse de nombreux systèmes de sécurité d'entreprises étatiques ou privées. A la même époque, l'entreprise américaine Adobe se fait subtiliser les données – mots de passe et informations bancaires – de 38 millions de clients! La chaîne de magasin Target fait une annonce similaire concernant 70 millions de clients... Le maliciel *Cryptolocker* crypte tous les fichiers stockés sur un disque dur et les supports externes de données qui sont raccordés, les rendant inaccessibles à l'utilisateur[6]. La technique du *phreaking* permet d'intercepter les messages de personnalités, de leurs proches que l'on peut ensuite faire chanter.[7]

Les spécialistes des technologies de l'information et de la communication parviennent parfois à remonter de belles pistes !

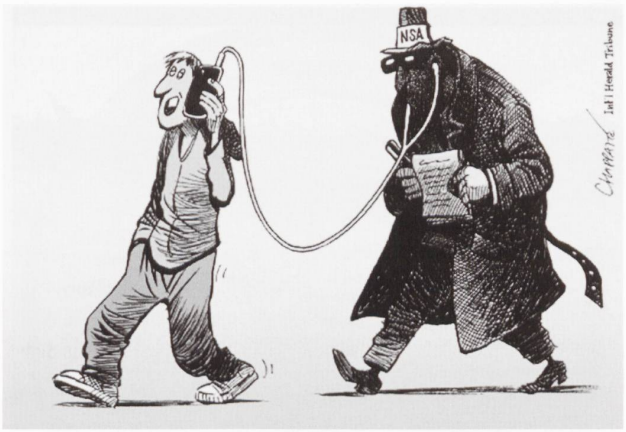
Sur un théâtre d'opération, neutraliser un radar grâce à l'informatique, non avec un missile, apparaît comme une bonne solution. Un virus, introduit en été 2011 dans le système d'information de la base de Creech, cloue au sol pendant une semaine la flotte de drones *Predator*. Un chercheur de l'Université d'Austin *attaque* un drone civil en lui faisant parvenir, grâce à une radio SDR du

4 http://www.opex360.com/201403/09/virus-informatique-puissant-ciblerait-lukraine/

5 Entre autres, le 1er RCP à Pamiers.

6 Confédération suisse: 18e Rapport semestriel MELANI.

7 Reuters, 3 décembre 2013.



commerce, de fausses informations GPS. Il existe des méthodes plus radicales à la portée de n'importe quel combattant, qui ciblent les drones militaires. Ce genre d'attaque s'avère peu efficace pendant le vol puisque, en cas de perte prolongée de signal, l'engin regagne automatiquement son point de départ. En revanche, le danger devient beaucoup plus grave, lors du décollage et de l'atterrissage[8].

Les forces armées américaines ont subi des attaques de ce genre, avec pour conséquences la perte de contrôle et la destruction d'un *Predator*, d'un drone *RQ-l70 Sentinel*, ainsi que d'un missile de croisière lors d'un tir d'essai aux abords de la mer de Chine. Les enquêteurs redécouvrent à cette occasion les travaux entrepris par certains hackers depuis une quinzaine d'années, sur l'intrusion dans des systèmes de communication lourdement chiffrés. En février 2009, des attaques visent les serveurs utilisés par le drone français *Harfang*, au début de son engagement en Afghanistan.

Les communications par satellites

Avec un ordinateur, une parabole, un décodeur Dreambox et quelques logiciels, presque n'importe qui peut accéder à des flux d'informations transmis par des satellites. Ceux-ci souffrent de multiples et graves *vulnérabilités*, donc de gros risques d'interceptions, de manipulations, de blocages, voire de prise de contrôle. Sont concernés les systèmes d'Inmarsat-C, Very Small Aperture Terminal (VSAT), Broadband Global Area Network (BGAN), BGAN machine-to-machine (M2M), FleetBroadband (FB), SwiftBroadband et Classic Areo Service, utilisés aussi bien pour la navigation maritime et aérienne que pour les communications militaires. Ces systèmes contiennent des portes dérobées, des protocoles mal sécurisés et insuffisamment documentés, des algorithmes de chiffrement trop faibles. Les terminaux satellites à large bande d'Inmarsat utilisent un « protocole de communication non sécurisé qui permet à des utilisateurs non authentifiés d'exécuter des opérations privilégiées sur les dispositifs. »

Un seul de ces systèmes étant contaminé, l'infrastructure entière des SATCOM risque de poser problème. Les navires, les avions, les militaires, les services d'urgence, les services des médias, les infrastructures industrielles (plateformes pétrolières, gazoducs, usines de traitement des eaux) n'échappent pas à ces vulnérabilités.

« *La menace augmente, et même de manière galopante. Pas une semaine ne passe,* souligne le contre-amiral Arnaud Coustillière, officier général français à la cyberdéfense, *sans qu'on parle d'une grosse attaque informatique ou d'une importante affaire de cyberespionnage. (...) Ce que l'on voit poindre aujourd'hui sont des attaques à fin de destruction (...)* [ainsi] *l'attaque sur Aramco en 2012 qui a mis hors service près de 30'000 postes informatiques. De plus en plus de nations développent des capacités offensives. Celles-ci font désormais partie des nouveaux systèmes d'armes que chaque pays veut posséder. C'est le cas notamment de l'Iran ou de la Corée du Nord.* »[9] Les cyberattaques seront de plus en plus destructives ![10]

Des secrets d'Etat sont-ils possibles dans le cyberespace ?

La toile ne manque pas de cyber-activistes qui cherchent à promouvoir leur cause ou leur idéologie à coups de divulgations plus ou moins sensationnelles. Depuis les premières révélations d'Edward Snowden, les programmes d'écoutes de la NSA et de ses alliés n'en finissent pas de faire la une de l'actualité et l'on en oublie les divulgations de *War Logs* et de télex diplomatiques en 2010 par WikiLeaks. A chaque fois, la même marque de fabrique: de prétendus lanceurs d'alerte portent, via internet, à la connaissance du monde des informations classifiées, cela avec le concours actif de grands titres de la presse écrite. Malgré les remous médiatiques, pas sûr que les nouvelles technologies modifient les rapports entre acteurs, qu'ils prêchent la transparence ou la défense de la raison d'Etat. Par ailleurs, celle-ci n'est-elle pas, le plus souvent, un mal nécessaire ?

Internet permet de dénoncer un secret, mais également d'apporter la preuve de son existence. Wikileaks en a fait le cœur de sa stratégie, Edward Snowden son *assurance-vie*. Pourtant, les briseurs de secrets n'ont pas les moyens de s'opposer véritablement à la puissance des Etats et des grands groupes industriels ! Les effets de leurs révélations sont difficilement évaluables. Au-delà d'une indignation passagère, quelle portée accorder aux actions de WikiLeaks ? Peut-on évaluer l'action des Anonymous dans les Printemps arabes ? Dix ans après le scandale ECHELON, le Gouvernement américain et la NSA n'ont pas été inquiétés, et l'on découvre avec l'affaire Snowden que leurs programmes d'interception ont été sensiblement améliorés. Si les programmes d'espionnage d'Etat ont toujours existé, ceux déployés par la NSA américaine surprennent par leurs capacités, des systèmes d'interception de millions de communications internet.[11]

H.W.

A suivre

8 *TTU* N° 932, 30 avril 2014.

9 *Le Point.fr* – publié le 29 janvier 2014.

10 Boris Manenti : « Une attaque informatique est une agression comme une autre », 23 janvier 2014 sur internet. Gilbert Kallenborn : « Les cyberattaques seront de plus en plus destructives », 4 octobre 2014 sur internet.

11 Jean-François Fiorina, directeur adjoint de Grenoble Ecole de Management: «Quel secret d'État dans le cyberespace?»