La cyberdéfense, nouveau front de guerre (2e partie) [Fortsetzung]

Autor(en): **Weck, Hervé de**

Objekttyp: **Article**

Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2015)**

Heft 4

PDF erstellt am: **26.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-781300

Au centre de la cyberguerre, les quartiers généraux du XXIe siècle.

Cyber

La cyberdéfense, nouveau front de guerre (2e partie)

Col Hervé de Weck
Ancien rédacteur en chef, RMS

« Une cyberattaque se lance toutes les secondes et demie... » La première partie de cet article est paru dans RMS No. 5, 2014, p. 5-8. »

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.

Des stratégies défensives qui ne sauraient ignorer l'offensive

Aux Etats-Unis

« Si vis *pacem, para bellum* ». Le général Keith Alexander, qui commandait en 2012 à la fois la National Security Agency et l'US Cyber Command, rappelait ce principe qu'il entendait l'appliquer à la lettre: « *Si votre défense consiste simplement à essayer de parer les attaques, elle ne peut pas être efficace. Parfois, le Gouvernement doit étudier ce qu'il faut faire pour stopper les attaques, pour les stopper avant qu'elles ne surviennent. Pour notre défense, nous devons aussi étudier de mesures offensives.* » Le droit international s'appliquant aux activités dans le cyberespace, une agression contre les systèmes informatiques devrait suivre les mêmes procédures d'engagement qu'une attaque militaire classique. On peut assimiler certaines cyberattaques contre les secteurs industriels stratégiques, les réseaux d'électricité, d'eau potable, de téléphonie dirigées par des Etats à un usage de la force et répliquer, en légitime défense, avec les mêmes moyens ou avec des forces militaires conventionnelles.

Les logiciels malveillants (*malwares*) américano-israéliens *Stuxnet* et *Flamme* semblent les première armes cybernétiques, qui ont infecté des dizaines de milliers d'ordinateurs au Moyen-Orient, dans le but de pénétrer quelques machines cibles. Depuis 2010, la National Security Agency dispose d'un programme « OWN INTERNET » qui automatise le piratage de dizaines de millions de machines dans le monde pour en exploiter le contenu. Dans la foulée, une unité de développement crée des *malwares* furtifs qui échappent aux antivirus du marché.

A l'insu de leurs utilisateurs, des ordinateurs, également des smartphones, enregistrent les mots de passe, contaminent les clés USB, afin de cibler les machines déconnectés des réseaux, activent à distance des micros et des webcams, bloquent l'accès à certaines données. Les usurpations par la NSA sur le site Facebook semblent avoir dopé le rythme de diffusion de ces *malwares* sur la toile. L'agence américaine s'intéresse particulièrement aux routeurs, aux réseaux téléphoniques, aux réseaux privés virtuels, aux réseaux d'entreprises ou d'administration. La pénétration du réseau belge Belgacom aurait permis d'infecter les téléphones de la plupart des hauts fonctionnaires de l'Union européenne.

Le système des systèmes de la NSA repose sur deux composantes, « TURMOIL » qui assure le suivi permanent de milliers de cibles, quel que soit le type de média utilisé, ainsi que « TURBINE » qui en automatise la pénétration et l'exploitation des données collectées. Il serait dès lors possible de constituer un grand tableau des intentions *adverses*, un objectif inaccessible aux analystes humains, trop dépendants de leur environnement immédiat.[1]

1 *TTU* N° 929, 9 avril 2014.

En Israël

Pour Israël, le danger dans le cyberespace s'avère aussi important que sur le territoire, aux frontières ou dans le ciel: les attaques, surtout à partir de Tunisie ou de Gaza, sont bien plus nombreuses sur internet. En janvier 2012, le hacker saoudien Omar s'en prend aux comptes bancaires de *l'ennemi juif* pour l'affaiblir financièrement et socialement. Il aurait piraté 400'000 identités bancaires, Tel Aviv en annonçant 14'000... Des Palestiniens et des Egyptiens s'en prennent au compte Facebook et au site officiel du premier ministre Benyamin Netanyahu, dont le portrait est remplacé par celui d'Hitler. Le piratage en novembre 2013 de 13'000 comptes Facebook pour « dénoncer l'occupation israélienne » se situe dans ce contexte. De telles attaques peuvent aussi bien provenir d'un individu, d'antisionistes quelque part dans le monde, de groupes de hackers comme Anonymous ou d'un Etat, entre autres la Chine.

Une cyberattaque, le 8 septembre 2013, provoque la fermeture, à Haifa, des tunnels du Carmel qui peuvent servir d'abris publics. Résultats: d'énormes perturbations, ainsi que des pertes s'élevant à des centaines des milliers de dollars. Un cheval de Troie a été introduit dans le système de caméras de sécurité de la route à péage des tunnels. Le lendemain, ceux-ci doivent de nouveau être fermés pendant huit heures. Attaque, semble-t-il, de pirates de haut niveau, mais pas assez sophistiquée pour provenir d'un gouvernement ennemi comme l'Iran[2].

La division technologique Lotem-C4I de Tsahal, créée en 2011, a une mission de cyberdéfense. Elle figure parmi les meilleurs au niveau mondial. Elle recrute des experts de l'Armée, ainsi que des professionnels sortant de l'ingénierie et des technologies de l'information, mais elle compte surtout sur des étudiants doués en informatique. Le service militaire, de trois ans pour les hommes, de deux ans pour les femmes, permet de tester leurs compétences, de sélectionner et d'utiliser les sujets les plus intéressants. Selon le lieutenant-colonel Eric, chef des technologies à la division Lotem, « *les jeunes de dix-huit ans qui l'intègrent arrivent avec des connaissances beaucoup plus avancées que ce que Tsahal possédait il y a dix ans.* »

Tsahal ne couvre pas ainsi tous les besoins. Une formation professionnelle d'entraînement à la cyberdéfense de plusieurs mois à l'Université de Tel-Aviv, baptisée «Cyber Bouclier» a donc été mise sur pied. Les participants peuvent ensuite intégrer l'armée de l'air, la marine, les renseignements ou la télégestion, mais une grande majorité d'entre eux rejoint la division Lotem. Ce recrutement ne dispense pas de prendre en compte des attaques internes comme, en 2011, l'affaire Anat Kam, ce soldat de Tsahal qui a donné aux médias des informations classifiées concernant la cyberguerre.

Les personnels de la cyberdéfense et la cyberattaque travaillent de concert dans un même lieu, 7 jours sur 7, 24 heures sur 24. L'équipe « ROUGE » attaque régulièrement d'une manière aléatoire l'équipe « BLEU » pour la tester. Elle conçoit elle-même ses virus, puisque les Etats, dans leurs opérations cyber, utilisent rarement des virus déjà connus. On tente ainsi de simuler au mieux les attaques auxquelles Israël pourrait avoir à faire face. Le Gouvernement de l'Etat hébreu refuse de dépendre de compagnies privées pour réfléchir sur la cyberguerre, concevoir des attaques, déployer des défenses. Les militaires israéliens travaillant dans le cyber, s'ils l'estiment nécessaire, ont le droit de ne pas répondre dans ce domaine à leur hiérarchie.[3]

Des chercheurs de l'Université Ben Gourion à Beersheva prétendent avoir trouvé en 2014 une méthode pour détourner des informations sensibles d'un ordinateur qui n'est pas relié à internet, une précaution que prennent les services de renseignement et les entreprises d'armement. On parvient à y introduire un virus en utilisant les ondes radio produites par l'ordinateur visé que réceptionne un téléphone portable. La National Security Agency américaine ne serait pas encore capable d'une telle performance...[4]

En Chine

La Chine se trouve régulièrement soupçonnée, voire accusée d'espionnage via les réseaux informatiques. Presque la moitié des cyberattaques identifiées dans le monde semblent imputables au 3e Département de l'Armée populaire de libération chinoise et à des agences étatiques civiles.

Les sociétés de télécommunications chinoises ZTE et Huawei proposent des produits compétitifs, parfois 20 % moins chers que leurs concurrents. Ils pourraient comprendre des dispositifs de surveillance, d'interception, voire un système permettant d'interrompre à tout moment l'ensemble des flux de communications. Le sénateur français Jean-Marie Bockel, qui craint des liens étroits entre ces deux firmes et le Gouvernement chinois, propose en 2012 de leur interdire le marché européen. Le comité d'intelligence de la Chambre des représentants américains en arrive aux mêmes conclusions, alors qu'une de ces entreprises exploite le réseau d'un important opérateur suisse de télécommunications. Des incidents bizarres seraient produits sur les réseaux d'entreprises américaines clientes de ces équipementiers...

Après plusieurs affaires d'espionnage contre l'Australie impliquant la Chine, ainsi que le piratage des réseaux de la Banque centrale, le Gouvernement de Canberra interdit à Huawei de faire une offre pour le programme national d'internet à bandes larges. En mai 2014, un serveur chinois semble avoir participé au piratage des plans secrets du futur siège des services secrets australiens: plan des étages, endroits où se trouvent les serveurs, disposition des câbles censés garantir la protection et assurer les communications. L'attaque a été menée contre un fournisseur participant à la construction du bâtiment[5].

2 Source: Koide9enisrael, publié par David Illouz.

3 *Mena Post*, janvier 2014.

4 *TTU* N° 938, 18 juin 2014.

5 AFP: «Le QG des services secrets d'Australie aurait été piraté par des Chinois», 28 mai 2014.

Même la défense cybernétique chinoise présente des failles. En octobre 2014, des hackers du mouvement Anonymous, opérant en soutien du mouvement contestataire à Hong Kong, réussissent pourtant à siphonner des sites internet de l'Armée populaire et d'une cinquantaine agences d'Etat chinoises. Ils récoltent des messages et des mots de passe par dizaines de milliers.[6]

En France

En 2008, le *Livre blanc sur la défense* identifie le risque d'attaques majeures contre les systèmes d'information comme une menace stratégique. La cybercriminalité représente un danger majeur dans tous les secteurs: criminalité de droit commun, terrorisme, espionnage et intelligence économique. Un véritable bilan des dégâts n'a jamais pu être établi car, sans oublier le « Secret Défense », de nombreuses entreprises ne souhaitent pas souffrir d'une contre-publicité.

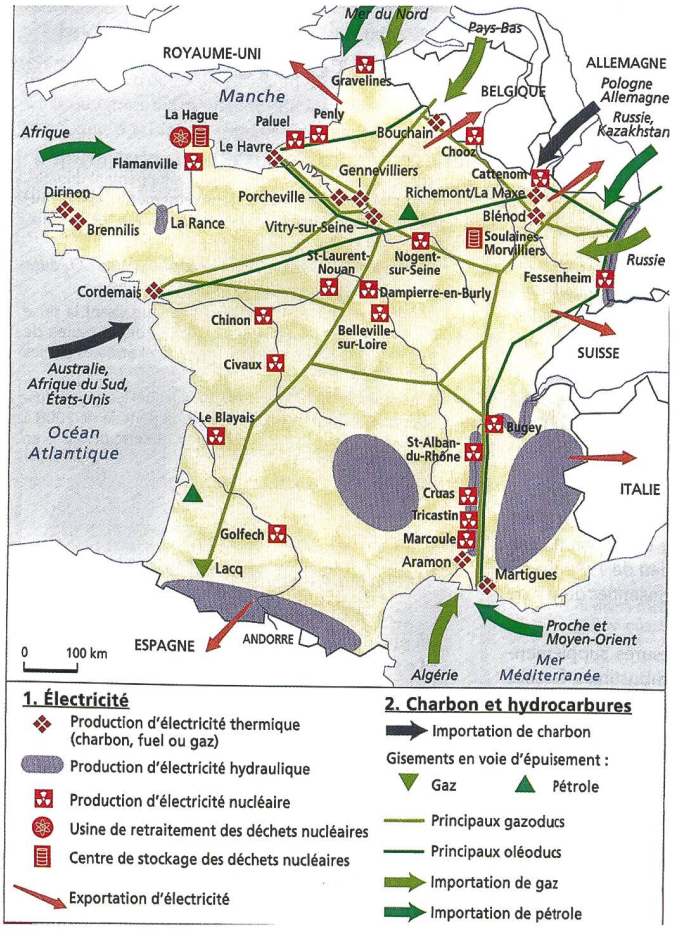
L'Agence nationale de la sécurité des systèmes d'information (ANSSI), créée en 2009, assume des missions de prévention mais aussi de réaction. Faute de ressources suffisantes, elle ne peut répondre à toutes les menaces. Son action ressemble à celle des pompiers: elle intervient auprès des administrations ou des grandes entreprises victimes d'attaques, pour les aider à gérer la situation. Depuis 2012, la France dispose d'une capacité offensive; elle peut considérer des cyberattaques importantes comme des actes de guerre. La Direction du renseignement militaire ne se trouve pas en pointe dans ce domaine, contrairement à l'ANSSI, à la Direction centrale du renseignement intérieur et à la Direction générale de la sûreté extérieure. A la direction nationale du renseignement et des enquêtes douanières, les bases de données, destinées à la surveillance du cybercommerce, représentent un poste budgétaire important. La cellule « Cyberdouane » dispose des moyens nécessaires pour développer des *coups d'achat* qui permettent, sous une identité fictive, de pénétrer les réseaux[7].

Alors que le Gouvernement socialiste parle de diminuer le déficit du budget et revoit sans cesse celui des forces armées à la baisse, un milliard d'euros, entre 2014 et 2019, devraient servir à défendre le pays contre les cyberattaques, à renforcer les personnels (550 postes) et à « accompagner des opérations militaires ». Pour tester sa cyberdéfense, l'Armée française a mis sur pied, du 1er au 3 octobre 2014, un exercice global « DEFNET », impliquant le haut commandement et des forces sur le terrain. Pourtant, pas question de jouer dans la même cour que les Américains!

Pour limiter les risques de cyberattaques ou de cyberespionnage, certains proposent de travailler avec des logiciels libres et d'abandonner Microsoft dont on soupçonne que les produits contiennent des programmes-espions, des *back-doors* utilisés par les services de renseignement américains. Des membres de la National Security Agency travailleraient dans des équipes de Microsoft. Pas si simple, répond le contre-amiral Arnaud Courtillière en charge de la cyberdéfense à l'Etat-major des armées! La coopération et les engagements multinationaux passent par Microsoft. D'autre part, quelle alternative lorsque le réseau compte des milliers de postes de travail? Par rapport aux autres opérateurs qui proposent un travail collaboratif, un environnement évolutif, des mesures lorsqu'une vulnérabilité est détectée, Microsoft s'avère le meilleur et ses systèmes ne sont pas plus faciles à attaquer que les logiciels dits libres. Il n'en reste pas moins que, pour se protéger véritablement, il faudrait faire cesser l'hégémonie de la technologie américaine et crypter toutes les communications, ce qui a un coût et ne peut être efficace qu'à l'échelle de l'Union européenne.

En cas d'offensive de grande ampleur menaçant la sécurité nationale, l'Etat doit compter sur une capacité de défense active qui lui permette de voir qui se trouve derrière l'opération et de répliquer avec tous les moyens dont il dispose, la meilleure réponse n'étant pas forcément une contre-attaque informatique. Une *règle militaire d'engagement* est nécessaire, qui détermine si on a le droit de *tirer*. Encore faut-il transposer dans le cyberespace les prescriptions relatives à la guerre conventionnelle ou asymétrique. En France, le travail est en cours, mais les organes impliqués, les solutions et les procédures resteront secrets. Le cadre juridique français sépare nettement les actions des services de renseignement et celles des acteurs de la cybersécurité,

Les infrastructures sensibles aux cyberattaques en Suisse et à l'étranger.



6 *TTU* N° 949, 15 octobre 2014.

7 Michel Cabirol: « Cyberdéfense: les espions vont disposer de capacités informatiques offensives», *LaTribune.fr*

alors que les Anglo-Saxons mélangent cyber sécurité et interceptions dans le cyberespace.

En Allemagne

Selon l'expert allemand Sandro Gayken, « *la Bundeswehr ne sait pas ce qu'est la Cyberwar,* » bien qu'elle dispose depuis le début des années 2000 d'un centre dédié à la cyberdéfense avec une soixantaine d'experts, ainsi que d'un institut de recherche sur la question à l'Université de la Bundeswehr. On teste les technologies militaires sous tous les angles, y compris l'ergonomie des postes de travail, mais jamais les équipements, les réseaux informatiques pour voir s'ils résisteraient aux attaques de hackers de haut vol. Les forces armées allemandes utilisent des ordinateurs – un peu mieux protégés que ceux d'une entreprise – et des programmes essentiellement basés sur des technologies vendues dans le commerce. Un service de renseignement étranger peut entrer très facilement dans ces réseaux, sans que personne ne s'en aperçoive[8].

En Suisse

Entre 2007 et 2012, les ordinateurs du Département fédéral des affaires étrangères subissent régulièrement des attaques, alors que la Suisse mène une médiation dans le dossier iranien. Cette situation décide le Conseil fédéral à faire coder la plupart des conversations et à s'exercer à déjouer une attaque cybernétique[9]. Des Etats étrangers, dont les Etats-Unis, surveillent et déclenchent des cyberattaques de manière ciblée contre des institutions, des organisations non gouvernementales, suisses et internationales installées dans le pays. Certaines de ces opérations vont en effet bien au-delà des possibilités de groupes de cybercriminels ou de *pirates*, surtout quand elles recueillent des données qui n'ont aucune valeur économique sur le marché gris, indice d'une collaboration entre des instances étatiques, des hackers, voire des criminels.

Pour contrer la menace liée aux nouvelles technologies, le Conseil fédéral adopte en juin 2012 une Stratégie nationale de protection de la Suisse contre les cyberrisques. La Centrale d'enregistrement et d'analyse pour la sécurité de l'information (MELANI) sert de plateforme d'information pour l'évaluation, la transmission, la coordination et la gestion des cyberrisques. A la fin 2017, elle assurera un rôle de direction opérationnelle. Un comité de pilotage, créé en 2013, coordonne les mesures prises dans l'administration fédérale, en collaboration avec les Cantons et l'économie.[10]

Même un Etat neutre peut envisager, dans le domaine de la cyberguerre, un partage des méthodes, une coopération en matière de plateformes ou d'expertise. L'Agence européenne de la Défense a reçu un mandat en ce sens en novembre 2013.

Pas facile de décider une cyberattaque !

Les puissances occidentales soutiennent le Gouvernement ukrainien – pas toujours irréprochable – en guerre contre les séparatistes pro-russes dans l'est du pays. La Crimée a d'ores et déjà été annexée par Vladimir Poutine. L'OTAN et les Etats membres n'ont pas la volonté et les moyens d'intervenir militairement dans le conflit. Pourquoi l'Alliance ne mène-t-elle pas, contre la Russie, une cyberattaque-punition qui respecterait les lois de la guerre ? Elle est à même de dégrader, d'infiltrer, de pervertir, de tromper les systèmes de communication de Poutine. Comme en Syrie et pour des raisons similaires, elle devrait s'abstenir.

Le choix des cibles s'avère délicat: faut-il s'en prendre à des infrastructures vitales en Crimée, en Ukraine, en Russie, sans faire, pour des raisons d'image, de victimes *innocentes*, a fortiori de *bons* Ukrainiens au lieu de Russes et de russophiles ? S'en prendre au dispositif militaire russe, à quoi bon si aucune armée occidentale n'intervient sur le terrain? Est-il efficace d'envoyer un message à Poutine qui a résisté à des menaces plus puissantes et qui dispose des moyens de riposte cybernétique ?

Il y a encore l'effet « Boîte de Pandore » ! Le président américain peut-il mener un cyberattaque conte une grande puissance, au moment où son pays se trouve impliqué dans l'énorme scandale de la surveillance planétaire par la NSA ? Ce serait mal se placer pour préconiser une gouvernance mondiale de l'internet face aux pays partisans de la souveraineté numérique. Les cyberattaques qui ne cessent de se multiplier contre leurs sites en incitent certains à vouloir créer des réseaux internet nationaux à l'abri des écoutes, des vols et des manipulations de données. Ils veulent retrouver dans ce domaine leur souveraineté et un véritable pouvoir de contrôle. Le Gouvernement allemand l'envisage comme son homologue brésilien. On parle également d'un réseau autonome pour l'Union européenne et les Etats-membres. En lançant une cyberattaque contre la Russie, Barak Obama favoriserait la *balkanisation* du Web.[11]

Un grand exercice du 3 au 21 novembre 2014

L'Armée, les corps cantonaux de police, les pompiers, les secouristes et la Protection civile, alarmés en même temps,doivent faire face à une catastrophe majeure, similaire à l'accident nucléaire de Fukushima le 11 mars 2011. En Suisse, le dernier exercice de défense générale a été mis sur pied en 1992, encore dans un contexte de Guerre froide.

Le scénario de l'exercice 2014 ,conçu par André Duvillard, ancien commandant de la police neuchâteloise et actuellement à la tête du Réseau national de sécurité, correspond à des menaces très actuelles sur une société moderne vulnérable: *black-out*, pandémie, cyberattaques, panne de courant à grande échelle et de longue durée. Si elle ne dure pas plus de trente-six heures, la population peut vivre avec, mais le problème, c'est de redémarrer le réseau, ce qui peut prendre des semaines.

8 http://www.ttu.fr/cyberwar-la-bundeswehr-est-elle impuissante/

9 Bertrand Fischer : « Une parade contre la cybermenace », *Le Quotidien jurassien*, 16 juillet 2013.

10 *La sécurité de la Suisse. Rapport de situation 2014 du Service de renseignement de la Confédération SRC*, pp. 69, 71, 77

11 François-Bernard Huyghe, directeur de recherche à l'IRIS: « La cyberguerre à laquelle vous échapperez peut-être aussi », 13 mars 2014.

La Suisse n'est pas un hérisson cybernétique, ni le Pentagone à Berne... ni les quartiers généraux de l'Armée.

Les entreprises, des cibles ?

L'installation et l'enclenchement de chevaux de Troie – des programmes-espions – se multiplient sur les réseaux où transitent des données sensibles, des échanges commerciaux, des plans de construction, des montages financiers, des comptes rendus d'expériences scientifiques. Des systèmes de contrôle permettent d'accéder à distance, pour les piloter, aux installations de distribution d'électricité, d'eau, de gaz, aux chaînes de production de l'industrie, aux réseaux bancaires. Sans mesures de protection adéquates, ils sont très sensibles aux cyberattaques.

Pour mettre à bas le système financier d'un pays, nul besoin de déposer des bombes dans les sièges centraux des banques, comme dans le roman *Fight Club* de Chuck Palahniuk. Il faut plutôt s'attendre à un scénario à la Tom Clancy dans sa série « Net Force. » Des cyberattaques, utilisant un *malware* quasiment indétectable, ont visé des banques américaines. L'opération provoque une paralysie de leurs services en ligne, des dénis de service dus aux cryptages d'opérations financières, gourmandes en ressources. Selon des experts américains, elles proviendrait d'Iran. Des cybercombattants d'Izz ad-Din al-Qassam, se disant indépendants de tout gouvernement, auraient revendiqué une de ces vagues de cyberattaques. A l'instar de la branche armée du Hamas, le nom de ce groupe fait référence à une figure du monde arabe de confession sunnite, alors que le régime iranien est chiite.[12]

Les pirates sur les réseaux d'entreprises sont-ils des hackers, des services étatiques ou des collaborateurs de l'entreprise, d'un ingénieur, cadre modèle le jour, pirate le soir, militant politique la nuit[13] ? Aujourd'hui, n'importe qui peut se procurer des virus ou des chevaux de Troie. Certains escrocs dans des pays africains exploitent le filon, s'intéressant aux données bancaires des naïfs. Les profits réalisés sont importants et le risque pénal encouru faible, d'autant que les enquêtes se heurtent aux différences de législation. Le troyen « ZeroAccess, » qui a infecté 9 millions de machines, a généré jusqu'à 100'000 dollars de recette par jour[14].

France: les secteurs d'activités nationales d'importance vitale selon le décret de 2006

Protection de la population
Santé
Gestion de l'eau
Alimentation

Vie économique et sociale
- Energie
- Communication
- Electronique
- Information

Transports

Finances

Industrie

12 « L'Iran dément être à l'origine de cyberattaques visant les banques américaines, » 15 janvier 2013.

13 Jean-Marc Leclerc, « Des PC aux mobiles, pirates d'Etat et anonymes frappent tous azimuts, » *Le Figaro*, 27 septembre 2013.

14 *Ibid.*

Des communications par satellites sont sensibles aux cyberattaques.

Au début 2014, l'Agence nationale française de sécurité des systèmes d'information définit les secteurs d'activités d'importance vitale, met au point une liste secrète de 218 opérateurs nationaux, publics et privés, à protéger en priorité, ainsi que les modalités pour en renforcer la cybersécurité. « Ce qui nous intéresse, c'est le command control *d'une centrale nucléaire, les aiguillages de la SNF, les systèmes vitaux d'un hôpital. Tout ce qui, en cas de sabotage, d'une infrastructure entraînerait une catastrophe.*[15] »

Comment détecter des infiltrations *malignes* dans un système? La compagnie nationale d'électricité d'Israël a lancé une formation à l'intention de ses ingénieurs, en collaboration avec CyberGym, une société de cyberdéfense fondé par des agents des services secrets israéliens, qui s'occupe de sécuriser des grandes sociétés telles que la compagnie du gaz, du pétrole, des compagnies de transport et autres sociétés financières. Israël se sait particulièrement vulnérable dans ce domaine, parce qu'il n'a pas d'accords électriques avec les pays voisins, l'ensemble de cette infrastructure essentielle dépend d'une seule entité.

Les entreprises suisses, grandes et petites, restent aujourd'hui très vulnérables en matière de protection des données. Le Service national de coordination de la lutte contre la criminalité sur internet a enregistré 9208 dénonciations en 2013, soit une augmentation de 12% par rapport à 2012. Le *mal* peut se propager d'une organisation à l'autre, à cause de l'interdépendance des infrastructures techniques et informatiques. Une panne dans l'alimentation en électricité, les télécommunications ou le marché financier risque de créer des effets en cascade domino.

Le Conseil fédéral a saisi les enjeux. Il existe une stratégie nationale de cybersécurité, mais la feuille de route et les ressources pour l'appliquer restent insuffisantes. Selon Gérard Vernez, délégué du Chef de l'Armée suisse pour la cyberdéfense, il appartient aux entreprises de se réapproprier leur souveraineté digitale et de définir leurs véritables besoins informatiques. L'Etat ne parviendra pas à subvenir à tous les besoins des entreprises. Chacune doit prendre conscience de ses responsabilités, car les problèmes commencent souvent chez l'utilisateur. Si les entreprises et les individus ne font pas leur travail à l'interne en matière de cybersécurité, les moyens de la Confédération, même les meilleurs, se trouveront submergés par des bagatelles et ne serviront à rien.

Des pièges pour les privés

En janvier 2013, un programme malveillant affiche sur l'écran des victimes potentielles une fausse page d'accueil du ministère français de l'Intérieur disant en substance à l'internaute qui est allé sur un site, souvent licencieux: « *Nous sommes la police et vous avez été pris. Payez deux cents euros sur-le-champ, sinon vous serez poursuivi pénalement.* » Il arrive que les hackers actionnent la webcam de la victime et la font apparaître en direct à côté de l'injonction. Et les gens paient... Les téléphones mobiles ne sont pas en reste: en France: 350'000 d'entre eux ont été infectés en 2012. Le *botnet Spamsoldier* commande aux appareils infectés d'envoyer de salves de 100 SMS par minutes. Un hacker de vingt ans, arrêté à

15 http://defense.blog.lavoixdunord.fr/archives/2014/01/22/temp-273a6a4fbc-17c7e656e5283e5f88b7d9-12616.html#more

Amiens, a contaminé 17'000 smartphones qu'il activait à distance pour leur faire composer des numéros surtaxés. Pour se renseigner sur une personnalité, la technique du *watering hole* (abreuvoir) permet d'attaquer un site généraliste auquel la cible se connecte régulièrement. Le virus infecte tous les utilisateurs, alors qu'un seul ordinateur va être fouillé de fond en comble.[16]

Conclusion

Il apparaît peu vraisemblable qu'on en arrive un jour à une cyberdissuasion similaire à la dissuasion nucléaire. Le cyberespace est en effet totalement *gris*, les moyens, dans ce domaine, apparaissent comme des armes d'emploi, non de non-emploi comme les armes nucléaires stratégiques et tactiques. Ils connaissent une prolifération galopante animée par des acteurs très divers, étatiques et non étatiques.

Les grandes puissances hésitent à déclencher des cyberattaques ou des cyberripostes. Faut-il en conclure qu'elles dépensent des milliards de dollars pour des moyens qu'elles n'utiliseront guère? Dans l'opération contre l'Iran, il y avait une logique, celle de retarder, grâce au virus *Stuxnet* plutôt que par des missiles, la nucléarisation de la République islamique. Les Russes ont bien maîtrisé la cyberguerre contre l'Estonie en 2007, la Géorgie en 2008.

En va-t-il de même pour les Américains à propos de l'Ukraine? La cyberarme, capable d'éviter des effusions de sang, qui correspond si bien à la vision *high tech* d'une guerre par écrans interposés, semble ne jamais trouver les bonnes cibles, au bon moment (il est trop tôt pour *dévoiler ses batteries* ou trop tard pour en rester au stade cyber). Cette arme du fort, qui devrait compléter sa supériorité militaire, sert surtout à ceux qu'elle est censée combattre, c'est-à-dire des Etats faibles qui n'ont ni les mêmes budgets, ni la même technologie que les Etats-Unis ou l'OTAN, des Etats proliférants, des Etats-voyous et, de façon générale, les ennemis de l'Occident.[17]

Face au cyberespionnage, certains Etats souhaitent créer des réseaux internet nationaux. Même le président du Conseil d'administration de Google, Eric Schid, déclarait au début 2013 prendre en compte l'introduction de contrôles étatiques sur les réseaux internet; les utilisateurs devraient demander l'autorisation de surfer sur des réseaux étrangers. Certains vont jusqu'à annoncer la disparition de l'internet actuel, absolument incontrôlable ![18]

Le problème de la liberté d'information est-il vraiment un argument porteur pour le maintien de la situation actuelle, quand on sait qu'en 2013 un quart de tous les réseaux internet dans le monde – essentiellement dans les Etats non démocratiques – ne sont pas libres?

H.W.

16 *Ibid.*
17 François-Bernard Huyghe: *op. cit.*
18 Hannes Grassegger: « Staaten steigen aus dem Web aus, » *NZZ am Sonntag*, 9 février 2014.

News

Bahreïn

Les diminutions à répétition des budgets de défense britanniques impliquent une diminution des forces déployées outremer. Ceci s'accompagne, comme pour la France et même les USA, à l'établissement de centres d'acquisition de renseignements dans les zones sensibles.

Durant les années 1990, les Français ont transformé leurs infrastructures à Djibouti, devenues un important centre pour l'acquisition de renseignements dans un site géopolitique essentiel – le détroit de Menab, au large du golfe d'Aden, contrôle le transit entre le canal de Suez et le détroit d'Hormuz. Depuis les années 2000, la présence des services d'écoute et de renseignement ainsi que le déploiement de forces militaires américaines ont détrôné leurs prédécesseurs.

En décembre 2014, le Secrétaire d'Etat britannique aux Affaires étrangères, Philip Hammond, a annoncé l'établissement d'une base militaire permanente dans le royaume de Bahreïn, entre l'Arabie saoudite et le Qatar. Il s'agit de la première base britannique installée à l'est de Suez depuis 1971. L'infrastructure, basée dans le port de Mina Salman près de la capitale Manama, coûtera quinze millions de livres sterling. Elle permettra de recevoir les destroyers et les porte-avions britanniques actuellement en construction. Plusieurs dragueurs de mines de la Royal Navy opèrent déjà depuis cette base.

Il va de soi que cette base constitue le cœur des capacités britanniques dans l'action contre Al Qaeda ainsi que l'Etat islamique.

En Grande Bretagne, l'opposition travailliste et les organisations de droits humains ont critiqué cette décision – en raison du soutien implicite à la monarchie de la dynastie al-Khalifa, qui règne depuis plus de 200 ans, et dont la presse britannique a plusieurs fois critiqué le manque d'ouverture démocratique et la répression contre les mouvements shiites pro-iraniens.

A+V