La sécurité de la Suisse en 2012... : des menaces nouvelles et multiformes peu ressenties dans l'opinion (2e partie)

Autor(en): **Weck, Hervé de**

Objekttyp: **Article**

Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2013)**

Heft [1]

PDF erstellt am: **13.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-514864

Les satellites font partie des systèmes « Grandes oreilles » des Etats-Unis. Les services secrets occidentaux recourent, eux aussi, à des moyens similaires.

Politique de sécurité

La sécurité de la Suisse en 2012... Des menaces nouvelles et multiformes peu ressenties dans l'opinion (2e partie)

Col Hervé de Weck
Ancien rédacteur en chef, RMS

Les cyber-armes sont-elles l'équivalent des armes nucléaires d'antan?

Le terme cyberware apparaît en 1992. Conduite par des ennemis étatiques ou non, la cyber-guerre s'en prend aux nouvelles technologies de l'information et de la communication, une menace grave qui plane sur les particuliers, les entreprises, les cartes de crédit, les réseaux bancaires, même non reliés à Internet , les services publics, l'Etat, partant la sécurité nationale! Elle évolue rapidement dans ses modes et ses moyens d'action, la diversité de ses cibles potentielles et la difficulté d'identifier l'agresseur. Le cyber-espace, après la terre, la mer, l'air, la stratosphère popularisée par la Guerre des étoiles, est la cinquième dimension où peuvent se déployer des stratégies et des forces.

En ce début de XXIe siècle, les nations, les Etats faillis également, les organisations terroristes et criminelles interviennent dans le cyber-espace. Dans son roman Dette d'honneur paru en 1997, Tom Clancy décrivait une déstabilisation de l'économie américaine par une attaque informatique contre Wall Street. En octobre 2011, les pirates informatiques Anonymous menacent de lancer une telle opération...

Les mobiles de cyber-attaques

Menace, conflit, terrorisme, sabotage, espionnage, criminalité organisée, activisme, vandalisme.

Quelques moyens de cyber-attaque

- Programmes malveillants (virus, vers, chevaux de Troie);
- Attaques par portes dérobées ou messageries (spams, phishing);
- Attaques sur les réseaux (sniffing, dénis de service à la suite de flux de messages émis par des ordinateurs-zombies);
- Attaques par des mots de passe (crackages, attaques par dictionnaires);
- Cartographies de réseaux (ping, balayages de ports, SNMP, Nessus);
- Intrusions (vols d'identité, élévations des privilèges, effacements des traces);
- Evasions (poisoning, spoofing);
- Reversengineering, cryptoanalyse, snarfing, cookies.

Dans *Foreign Affairs*, William Lynn, secrétaire adjoint à la Défense américaine, évoque le seuil que les Etats-Unis ont franchi en matière de cyber-défense avec l'opération BUCKSHOTYANKEE. Il dévoile également certains aspects de la première attaque contre le système informatique du Pentagone, œuvre d'un service de renseignement qui a réussi à insérer une carte-mémoire contenant un code malicieux dans un ordinateur portable de l'armée américaine au Proche-Orient. En mai 2011, des données américaines, parmi les plus sensibles sont forcées: comptes Gmail de hauts fonctionnaires, plans de matériels militaires chez Lockhedd Martin. Les services de contre-espionnage y voient la main chinoise. « Cette intrusion en 2008 n'est pas la seule pénétration réussie. Des ennemis ont obtenu des milliers de dossiers des réseaux informatiques aux Etats-Unis, de leurs alliés, des formes aéronautiques, y compris des plans d'armes, d'opérations et des données de surveillance. » En octobre 2011, une station de contrôle d'un drone Predator, opérant sur la base de Creech (Nevada), subit une infection par virus, en dépit du fait qu'elle n'était pas reliée à Internet.

Cyber est le raccourci de cybernétique. Pour une approche surtout théorique de la cyber-défense, voir Gérald Vernez; Roman Hüssy; Riccardo Sibilia: « Cyber Defense der Schweiz », *Military Power* Revue der Schweizer Armee Nr. 1, 2/2011. Gérald Vernez: «Cyber Defense der Schweiz – Vor was muss siche die Schweiz schützen? 1.2.3.4.», *Allgemeine Schweizerische Militärzeitschrift* 5, 6, 7, 8/2012.

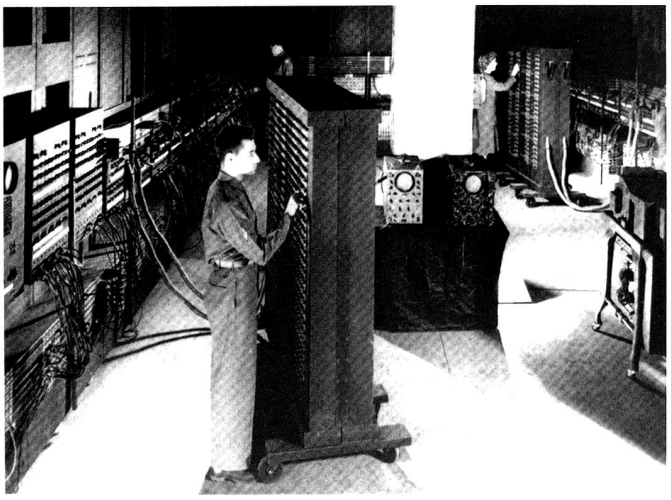
IRIS: Le cyber-espace, nouvel enjeu stratégique. Colloque du 18 septembre 2012.

Les gravures d'une puce sont tellement fines qu'on ne peut pas la démonter pour reconstituer ses circuits intégrés, d'où la difficulté de déceler les portes dérobées.

Face à une menace asymétrique dont l'origine s'avère impossible à déterminer, le US Cyber Command, nouvellement créé, protège l'ensemble des réseaux informatiques des forces armées et rationalise les moyens de lutte cybernétique. Les Etats-Unis ne sauraient se contenter de se replier derrière une ligne Maginot ! Le *New York Times* du 1er juin 2012 révèle que Barack Obama, dès ses premiers mois de présidence, a ordonné d'accélérer les cyber-attaques – initiées sous l'administration Bush Jr – contre les systèmes informatiques des installations nucléaires iraniennes. Un élément du programme, rendu public par inadvertance en été 2010 en raison d'une erreur de programmation, aurait permis au ver Stuxnet de s'échapper de l'usine iranienne de Natanz. Elaboré aux Etats-Unis et en Israël en 2006, lancé en 2009, lui et ses créateurs sont révélés en 2012 . En associant Israël au développement de Stuxnet, les Américains obtiennent que l'Etat hébreu n'attaque pas l'Iran et retardent d'au moins deux ans la naissance de la capacité nucléaire des ayatollahs.

Le général Keith Alexander, à la tête de l'US Cyber-Command et de la National Security Agency, soutient le 6 octobre 2012 qu'une cyber-attaque dirigée par certains pays pourrait être assimilée à un usage de la force. Dans un tel cas, le droit international s'applique et les Etats-Unis peuvent répliquer en état de légitime défense, soit en recourant aux mêmes moyens, soit en engageant des forces militaires conventionnelles. Mais pas question de déployer la grande armada lors d'attaques en déni de service ou de simples intrusions dans des systèmes informatiques. En revanche, riposte possible dans le cas où des infrastructures vitales sont visées (réseaux d'électricité, d'eau potable et de téléphone, industries stratégiques). Keith Alexander rapporte-t-il l'intention de l'administration américaine ou fait-il dans la dissuasion ?

...à l'écoute et au brouillage, au décryptage des messages amis et ennemis, parfois grâce à des ordinateurs encore balbutiants. Ici un Electronic Numerical and Computer américain en 1946.-



Océane Zudelbia : *Histoire des drones*. Paris, Perrin, 2012, p. 146.

J.H-R.: *Foreign Affairs*, volume 89, numéro 5.

Stephane Trano : « Virus Flamme, Stuxnet, drones, la CIA résiste aux enquêteurs », 9 juin 2012.

IRIS: op.cit.

En été 2012, chevaux de Troie, vers et virus informatiques font la une des médias occidentaux, avec des informations sur Stuxnet et Duqu. En revanche, on parle moins des firmware, ces logiciels qui équipent entre autres les routeurs, les imprimantes et qui sont rarement actualisés. On peut facilement y cacher des portes dérobées.

Flamme, programme malicieux de cyber-espionnage le plus complet découvert jusqu'à présent, touche surtout les particuliers et les universités. Il ne se réplique pas et ne détruit pas, il ne peut donc être considéré comme un virus. Il active des microphones lorsqu'il détecte à proximité des appareils Bluetooth, effectue des captures d'écrans en cas d'utilisation d'applications jugées intéressantes. A travers un réseau de serveurs qui empêche de remonter jusqu'à eux, les utilisateurs de ce programme accèdent à des informations contenues dans des centaines d'ordinateurs infiltrés ; ils peuvent l'adapter en fonction de l'intérêt de chaque machine. Moins sophistiqué que Stuxnet et Duqu, Flamme pousse à s'interroger à cause du choix de ses proies. Vraisemblablement développé par un Etat – la connexion établie entre ce maliciel et Stuxnet tendrait à l'indiquer – il ne se concentre pas sur l'Iran mais touche l'ensemble de la planète, dont Israël systématiquement suspecté dans les affaires de cyber-guerre.

Des Etats recourent-ils à des cyber-offensives non sélectives contre les réseaux alors que, jusqu'à présent, il ne s'agissait que de dommages collatéraux dans le cadre d'opérations très ciblées. Le phénomène-guerre se trouverait-il remis en question ?

Les barbouzes d'EDF

Les logiciels de type « Cheval de Troie » sont facilement téléchargeables sur Internet. La seule difficulté consiste à les installer correctement, et surtout à les rendre indétectables aux anti-virus. Le jeune informaticien Alain Quiros s'y emploie avec brio. Il lui suffit d'une adresse mail et d'une liste de mots-clefs pour siphonner entièrement un disque dur et en extraire toutes les informations nécessaires. Une technique quasi infaillible qui lui a permis de multiplier les piratages pour le compte de Thierry Lohro. Ancien du 13e régiment des dragons parachutistes, ce dernier a effectué une partie de sa carrière d'agent secret au Service « Opérations » de la DGSE avant de fonder sa propre société, Kargus, spécialisée dans « l'intelligence économique et la gestion de risques. »
De nos jours, ordinateurs, réseaux, téléphones portables et techniques électroniques ont pris une place prépondérante. Les réseaux de distribution d'électricité et d'eau fonctionnent grâce à eux, ce qui est susceptible de donner des sueurs froides quand on imagine leur vulnérabilité face à des pirates informatiques. Leur neutralisation aurait des conséquences incalculables sur la population visée.

Aussi, l'US Air Force a confié à la division Phantom Works de Boeing le soin de développer une nouvelle arme qui, appelée CHAMP (Counter-electronics High-Powered

Microwave Advanced Missile Project), se présente sous la forme d'un missile qui émet des salves de micro-ondes à haute puissance. Cela a pour effet de rendre inopérant tous les équipements électroniques situés dans un secteur donné.

Le 16 octobre 2011, ce missile a été testé dans l'Utah, sous la supervision de l'U.S. Air Force Research Laboratory (AFRL). Et les résultats ont été concluants car tous les ordinateurs et les systèmes électriques situés dans les sept immeuble expérimentaux survolés par l'engin ont été neutralisés, y compris les caméras qui y avaient été placées pour suivre l'expérience. Et le tout, sans causer le moindre dommage aux bâtiments.

« *Cette technologie marque une nouvelle ère dans la guerre moderne*, a estimé Keith Coleman, le responsable du programme CHAMP à la division Phantom Works de Boeing. *Dans un proche avenir, cette technologie pourra être utilisée pour rendre les systèmes électroniques et les données d'un ennemi inutiles avant même l'arrivée des premières troupes ou des avions*, » a-t-il ajouté.

Des principes de cyber-stratégie

Contournement et asymétrie

Dans une guerre conventionnelle, l'effort vise à obtenir un rapport de force favorable et à découvrir le point faible du dispositif ennemi; dans une cyber-guerre, des combattants, peu nombreux et pauvres en moyens, n'ont pas besoin de tester l'ensemble du système visé, ils cherchent des failles; dès qu'ils en ont trouvé une, ils y appliquent toute leur puissance de feu. La cybernétique a un pouvoir égalisateur: un individu peut mettre à mal un dispositif hyper-sophistiqué. Avec un drone coûtant trois cents euros, les chercheurs du Stevens Institute of Technology ont mis au point un système qui permet le piratage (*hacking*) de réseaux wi-fi faiblement protégés.

La territorialité apparaît comme un paramètre de moins en moins important. La révolution arabe a incité le gouvernement égyptien à isoler le pays d'Internet. Les quatre opérateurs, proches du pouvoir, coupent les connexions mais de petits malins, aidés par les Etats-Unis, réussissent à faire sortir des vidéos compromettantes sur l'ampleur et la répression des manifestations. Ce n'est pas un hasard si la Chine développe un moteur national de recherche Baidu, l'équivalent de Google, ainsi que des équivalents de Facebook et de Twitter. Les autorités espèrent ainsi garder la souveraineté sur l'information. Elles parviennent, pendant quelques jours, à bannir de leur moteur de recherche les réponses à certaines requêtes. Il n'en reste pas moins qu'un régime autoritaire, même totalitaire, qui n'abrite que des réseaux limités, ne parvient pas à exercer un contrôle total sur l'information. Dans le cyber-monde, les frontières s'avèrent poreuses!

Ambiguïté

Dans un cyber-conflit, l'agresseur signe rarement ses œuvres, et l'agressé n'arrive pas à l'identifier avec certitude. Preuves en soient la cyber-attaque contre l'Estonie en 2007 ou le virus Stuxnet en 2010. On est en droit de se méfier des logiciels de l'omniprésent Microsoft. L'entreprise refuse de publier ses codes-sources pour entraver la concurrence mais, dans la foulée, on ne peut savoir si elle fait ou pas de l'espionnage en amont. Les Russes développent d'ailleurs un système d'exploitation national basé sur Linux.

Primat de l'offensive

Le fait que l'agresseur peut rester caché favorise l'offensive mais pas la contre-offensive, les possibilités de contre-intrusion étant faibles. L'indispensable défensive demeure toujours inachevée et en renforcement.

Arme à double tranchant

Une cyber-offensive, comme une attaque chimique ou bactériologique, peut se retourner contre ses initiateurs. Des Etats parviennent à mettre au point des programmes malicieux d'excellente qualité, mais il leur est très difficile de contrôler une infection informatique, dès qu'elle est sortie du laboratoire. Stuxnet ne devait cibler que les ordinateurs des centrifugeuses iraniennes, mais quelques lignes de code l'ont répandu sur la toile mondiale. Le programme détecté et analysé, risque d'être utilisé par d'autres cyber-combattants qui peuvent encore le modifier.

Développer de tels programmes, c'est un peu créer un nouveau missile sol-air révolutionnaire, en équiper ses troupes et placer en téléchargement libre les plans et le manuel d'utilisation sur son site web, avec un numéro vert grâce auquel chacun peut commander le matériel nécessaire et être livré gratuitement.

Les Américains renoncent...

En 2003, le commandement américain envisage une cyber-attaque contre des banques irakiennes afin de priver Saddam Hussein de ressources financières, ce qui devrait accélérer la chute du régime sans faire parler les armes. L'administration Bush jr y renonce, prenant en compte les dommages collatéraux d'une telle opération sur l'ensemble des banques du Moyen Orient, voire de l'Occident.

Lors de l'intervention contre la Libye du colonel Kadhafi, le Pentagone ne lance pas une cyber-attaque contre la défense aérienne du dictateur, préférant tirer une centaine de missiles Tomahawk. Cette décision s'explique par le manque de temps: il faut faire vite pour secourir les insurgés, alors qu'une cyber-offensive exige une identification des points d'entrée, une analyse des systèmes et des vulnérabilités, l'écriture d'un logiciel malicieux, des opérations longues et compliquées.
Selon un expert américain, « une cyber-guerre pourrait gêner mais non désarmer un adversaire. Et n'importe quel adversaire a la capacité de frapper en retour d'une façon qui serait plus que gênante. » En Estonie, contrairement à ce qu'on a pu prétendre, les dommages

Claire-Marie Selles: « Cyber-guerre, le génie a-t-il jamais été dans la bouteille? », 21 juin 2012.

Slate.fr: « Les nouveaux barbouzes: quand le espions passent au privé », 18 octobre 2012.

en 2007 ont été assez légers, parce que le pays possédait sur son territoire un nœud-réseau qui a permis de rétablir les accès au plus vite.

Coalescence
Des individus s'assemblent hors de toute structure et mènent des actions groupées dans le cyber-espace. Elles peuvent être positives : des acteurs individuels ont pallié l'effondrement du système Internet haïtien après le tremblement de terre et l'ont fiabilisé en l'absence de toute intervention publique. Mais il peut s'agir de collectifs dangereux et militants, comme Anonymous ou Wikileaks. Dans une perspective plus conflictuelle, des groupes de hackers, alliés de circonstance, éventuellement commandités par un gouvernement, agissent contre un Etat, une institution, une grande entreprise privée. Ils bénéficient temporairement d'un rapport de force symétrique.

Fugacité
Une attaque ne se prolonge pas dans la durée, car une faille, généralement, est rapidement colmatée. Par instants, la défensive sera percée mais elle tiendra malgré tout durablement. Trente-cinq pays, selon l'enquête du CSIS, développent une doctrine militaire destinée à faire face à une cyber-guerre. Les grandes puissances mettent à jour leur stratégie de cyber-défense qui comprend naturellement un volet offensif secret.

Une cyber-défense pour la Suisse ?

Une petite puissance comme la Suisse, faute de crédits et de volonté politique, peut-elle renoncer à une cyber-défense ? Le Rapport sur l'Armée 2010 ne parle pas de cyber-guerre et, par conséquent, ne propose aucune mesure alors que, dans le pays, le nombre des cyber-attaques s'accroît. La Centrale fédérale pour la sûreté de l'information note le3ur nette professionnalisation et un changement au niveau de leurs mobiles: « *Les actes de vengeance, la volonté de nuire à la concurrence ou les agressions à motifs politiques ont pris le relais du simple vandalisme.* » Des pirates suisses s'en prennent aux sites des grands partis politiques, dont quatre ont été mis temporairement hors service à fin novembre 2010. Les auteurs, non identifiés, ont le profil d'ingénieurs agissant pour des raisons idéologiques. L'espionnage vient plutôt de l'étranger. Il y a encore les groupes organisés, installés en Europe de l'Est, qui utilisent des structures sophistiquées pour escroquer de l'argent ou pour louer des services de piratage. Des Suisses collaborent avec eux en ouvrant des comptes. Ils réceptionnent les sommes obtenues par arnaques, viennent les chercher au guichet et les expédient *via* Western Union, prélevant une commission au passage. En 2011, les attaques contre les grandes entreprises restent minoritaires. Sur les 885 incidents signalés, 75 % concernent des entreprises occupant moins de 1'000 salariés. Les PME sont moins sensibilisées à la sûreté de l'information que les grandes entreprises, d'où leur vulnérabilité.

Deux scénarios parmi d'autres

Une conférence internationale a lieu à Genève, les avions des délégations se suivent en ordre serré, les états-majors suisses mettent en œuvre leurs planifications pour assurer les mouvements et la sécurité des délégations. Voilà que, mystérieusement, le système Skyguide, les réseaux de conduite et de transmission, civils et militaires, les numéros d'urgence tombent en panne, comme l'alimentation de la ville en électricité et le système informatique des banques. Plus de bancomats! Les médias du monde entier montrent une Suisse incapable de remplir sa traditionnelle mission de bons offices. Voilà le résultat d'une cyber-attaque dont on ne découvrira jamais les auteurs.

Octobre 20... Après plusieurs mois de tensions autour d'un différend fiscal, le pays X lance une cyber-offensive contre la Suisse. Plusieurs terminaux de commandes centralisées des CFF subissent les effets d'un ver informatique qui corrompt les données montant des aiguillages, si bien que les indications déportées ne sont plus fiables. Dans le même temps, plusieurs usines électriques interrompent leur production, car un virus s'en prend aux commandes informatisées des conduites forcées et des circuits de vapeur des centrales nucléaires. Une partie importante des entreprises et de la population se voient privées d'électricité, puisque les capacités restantes sont monopolisées par les infrastructures étatiques et militaires. Interruption également du trafic aérien, civil et militaire, parce qu'un virus de type bombe logique paralyse les infrastructures du contrôle aérien. Il faut élaborer les cartes-mémoires contenant les plans de vol depuis d'autres bases, les acheminer à la bonne place, ce qui ralentit considérablement les opérations aériennes. Plusieurs quartiers généraux des autorités politiques et de l'Armée restent muets pendant des heures, suite à la mise en défaut des circuits de contrôle du conditionnement d'air par un malware. La chaleur dégagée par les ordinateurs, en particulier dans la salle des serveurs, ne peut plus être absorbée, d'où des arrêts intempestifs à répétition qui nécessitent de longs redémarrages. Confronté à des difficultés logistiques critiques, amputé d'une partie de ses moyens, face à un mécontentement croissant de la population, que peut faire le Conseil fédéral ?

En Suisse, on manifeste souvent une naïveté déconcertante dans les domaines du contre-espionnage et de la cyber-défense, partie intégrante d'une politique de sécurité. Cette dernière commence dans les foyers où il faut défendre ses données et celles de sa famille en appliquant avec sérieux les mesures de sécurité informatique. En service militaire, on respecte les directives concernant les informations sensibles et classifiées. Lors d'un exercice de troupe ou d'état-major, combien de clés USB sont

Océane Zubeldia : *op. cit.*, pp. 177-178.

Olivier Kempf en ligne, 18 février 2011. Marie-Claire Selles : *op. cit.* Sandro Arcioni : « La Cyberwar ou la guerre des temps modernes », *EclairaGE* 3/2011. Nathalie Guibert : « Le cyber-espionnage, une arme militaire et économique », *Le Monde géo et politique*, 21 décembre 2011.

Loïc Delacour, *Le Matin*, 21 avril 2011.

Ces scénarios sont une adaptation de ceux publiés par le commandant Damien Gadiou, Défense nationale et sécurité, « Cyberdéfense: passer à l'offensive ? – *Tribune* No 264 » et par Sandro Arcioni, *op. cit.*

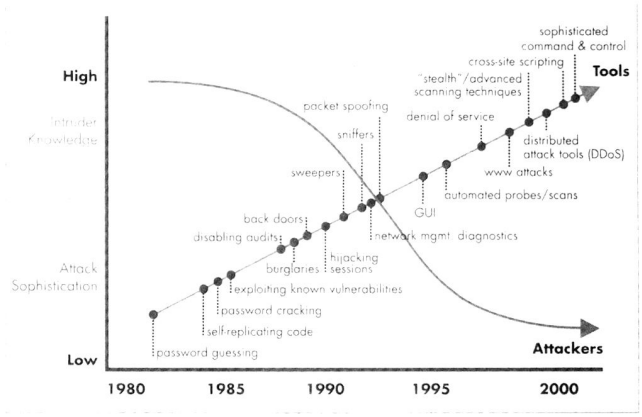
utilisées, combien d'appels lancés sur des téléphones non cryptés, combien de connexions à Internet depuis des postes contenant des données sensibles? Quel chemin à parcourir avant de garantir la sécurité de l'information opérationnelle, ce que les initiés dénomment OPSEC! La priorité reste à la protection basique des systèmes d'information. Nombre d'attaques exploitent des portes ouvertes et s'expliquent par le fait que les réseaux, en Suisse et ailleurs, sont très mal protégés. Pour les réseaux sensibles, cryptés et dupliqués, l'effort doit porter sur une surveillance active à même de limiter au plus vite l'effet d'une intrusion. Dans notre armée de milice, la cyber-défense s'avère plus difficile qu'ailleurs: en plus des serveurs officiels, un nombre élevé de moyens privés servent à stocker et à gérer des données sensibles, une situation idéale pour un agresseur. Il y a encore le travail à domicile sur des ordinateurs forcément moins protégés que ceux des entreprises.

Il faut donc une coopération étroite et sans arrière-pensée entre la Confédération, les cantons, les grandes communes, les décideurs politiques, les secteurs publics et privés, les acteurs de la sécurité informatique. Elle concerne l'armée, la justice, la police, les services de renseignement, la protection civile, le ravitaillement du pays. Il s'agit d'assurer les fonctions vitales, dont dépendent la sécurité cybernétique et la prospérité de la Suisse, grâce à un système adapté de prévention, d'anticipation, de dissuasion et d'intervention .

Le projet « Cyber-Défense » suisse, présenté comme une stratégie globale, ne prévoit pas une nouvelle agence fédérale mais une cellule destinée à coordonner tout ce qui se fait dans le domaine. Elle serait conçue à l'image du Réseau national de sécurité, chargé d'assurer la coopération entre l'armée, les pompiers, les hôpitaux etc., qui conduira en 2013 un grand exercice de conduite stratégique comprenant un scénario d'attaque des réseaux de communication. Le projet vise aussi à créer un corps de milice d'aide en cas de catastrophe cybernétique, intégrant des volontaires au sein des entreprises, chargés de faire remonter les informations, partager les compétences, voire de mobiliser en cas d'attaque massive.

Et qu'importe que la cellule soit rattachée au Département de la défense ou à celui des finances qui coiffe déjà un organe d'analyse et de sécurité informatique, MELANI, fort de huit personnes. Elle comprend deux réseaux d'une centaine de partenaires, dont l'un, fermé, regroupe les exploitants d'infrastructures nationales critiques. On y échange des informations provenant des services de renseignement et de la justice .

Contrairement à ce que donne à penser l'article de Gérald Vernez, Roman Hüssy et Riccardo Sibilia – il recommande le dialogue avec des Etats étrangers, l'ONU, l'Union européenne, l'OTAN et l'OSCE – la coopération internationale dans le domaine de la cyber-défense pose un problème de fond. Dans quelle mesure la Suisse peut-elle compter sur les bonnes intentions, ainsi que l'honnêteté de tels partenaires? On éprouve de forts doutes si l'on prend en compte l'espionnage économique



Le type d'attaque s'est modifié au fil des décennies. Les recherches ludiques de mots de passe d'autrefois sont remplacées aujourd'hui par la prise de contrôle «hostile» régulière de la totalité d'un réseau. Et ces attaques sont dangereuses, même si elles sont perpétrées par des personnes moins bien formées mais disposant d'outils logiciels sophistiqués.

Evolution de la cyber-menace en Suisse.

et le fait qu'en période de crise économique au sein de l'Union européenne et du monde occidental en général, des Etats démocratiques sont prêts à recourir à n'importe quels expédients, même illégaux, pour récupérer de l'argent dans un petit Etat dont ils n'acceptent pas le niveau de richesse. La cyber-défense est-ce un domaine dans lequel la Suisse doit faire dans l'Alleingang?

H. W.

Guillaume Baudoin: «La militarisation de l'Internet,» *EclairaGE* 3/2011

Gérald Vernez; Roman Hüssy; Riccardo Sibilia: op. cit.

Melde- und Analysstelle Information Assurance.

Yves Petignat: «La cyber-défense passera en mains des civils,» *Le Temps*, 5 mai 2012.