Les enjeux de la cyber-sécurité : répondre aux nouvelles menaces : oui, mais comment?

Autor(en): **Arcioni, Sandro**

Objekttyp: **Article**

Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2012)**

Heft 6

PDF erstellt am: **26.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-514713

Les conférences et les infrastructures critiques (ici le WEF à Davos) nécessitent une protection contre des menaces physiques, mais également une surveillance et une défense électronique.

Cyber-défense

Les enjeux de la cyber-sécurité : Répondre aux nouvelles menaces. Oui, mais comment ?

Lt col Sandro Arcioni

Ing. ETS/epg EPFL ; Dr. ès Sc. ; EM cond A

On parle d'attaques informatiques, d'attaques cybernétiques, de cyber-terrorisme, de « Cyber-war » ... Il y a une grande confusion dans ces différentes attaques. Dans un premier temps, il s'agit de segmenter l'approche afin de mieux comprendre le « pourquoi » et le but de ces attaques. Pour cela, nous allons grouper ces attaques en une typologie de quatre axes :

L'axe économique

Les « attaques économiques » visent les entreprises dans le but de les affaiblir, de les bloquer ou de les ralentir ainsi que de leur voler de l'information, un procédé de fabrication, un brevet, etc. dans un but de concurrence, de compétitivité entre entreprises. Ce type d'attaques relève de l'intelligence économique.

L'axe criminel (cyber-criminalité)

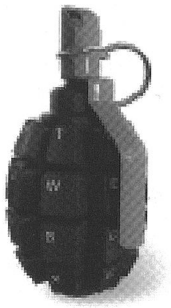
Les attaques à buts criminels relèvent de la « cyber-criminalité » et se séparent en deux sous-groupes distincts :
a. Les criminels agissant dans différents secteurs avec des profits très différents en fonction des types d'activités criminelles. Les secteurs visés :

- le crime organisé ;
- l'espionnage ;
- le blanchiment d'argent ;
- la contrefaçon ;
- les réseaux de prostitution ;
- les réseaux pédophiles ;
- l'usurpation d'identité, le vol (cartes de crédits, numéros de comptes bancaires, compte de loterie, etc.) ;
- les fraudes, les arnaques ;
- les trafiqueurs de paris en ligne (domaine du sport, loteries, etc.) ;
- etc.

Des informaticiens peu scrupuleux agissant sous forme de « BotNet » assurant ainsi « le routage » des données des criminels afin de faire disparaître toutes traces sur leurs origines, avec des profits, par contre, très importants. Ce sont aussi, par exemple, des « Advanced Persistent Threat » au profit d'un Etat, travaillant par scénarios. Ils sont difficiles à déceler et à juger (pas de bases légales). Ces informaticiens peu scrupuleux conçoivent de petits logiciels (BotNet), comme une plateforme de routage, permettant aux criminels du Net de faire transiter leurs données (spams, virus, cheval de Troie, etc.) par un très grand nombre de serveurs. Ils deviennent propriétaires de ces « nœuds de routage » répartis dans le monde entier à l'insu de tous. A chaque passage d'une donnée par un « nœud de routage » une somme est facturée à l'émetteur équivalant à 10 centimes d'euro. Plusieurs d'entre eux agissent au profit d'un Etat, par scénarios impliquant des « Advanced Persistent Threat » et utilisant les « BotNet » pour envoyer un « malware » ! (Ex : « Stuxnet ») dans le but d'être plus efficaces, de gagner plus d'argent et d'être le moins visibles possible en utilisant l'Internet.

Ce type d'attaques relèvent des services judiciaires de la police, d'Interpol, etc.

L'axe terroriste (cyber-terrorisme)



Il s'agit d'attaques informatiques provoquées par des groupes d'individus organisés en réseaux (ou non), sans avoir forcément un lien direct entre eux, mais poursuivant un but commun: les actions terroristes. Ces attaques sont équivalentes à des attentats, mais sans moyens logistiques lourds: déraillements de train, chutes d'avion, chantages, pressions provoqués par des logiciels malveillants. Ces activités criminelles dépendent des services judiciaires de la police, d'Interpol et de la sécurité d'Etat (si l'Etat est pris pour cible).

Les attaques à buts «politico-militaires» (Cyberwar)

La cyberwar n'est pas si différente dans la technique utilisée que le cyber-terrorisme, mais elle est très différente dans les buts recherchés, la façon de conduire la «guerre» et l'origine des attaquants. Il s'agit de groupuscules (Basque, Islamiste, etc.) ou un Etat (Lybie, Chine, Russie, Israël, etc.) qui, sous le couvert de l'anonymat, attaquent un Etat (Estonie, Iran, Suisse, etc.) ou les intérêts de ce dernier, dans le but de l'affaiblir, de le bloquer ou de l'anéantir. En Cyberwar, une cyber attaque est portée sur:

- les systèmes d'armes d'un pays;
- les réseaux électriques;
- les centrales nucléaires;
- les réseaux de télécommunication;
- les réseaux ferroviaires et/ou aériens;
- les réseaux informatiques de l'administration nationale de l'Etat;
- etc.

mais toujours en poursuivant le but d'affaiblir, de bloquer ou de paralyser un Etat. Ceci relève d'une responsabilité d'Etat qui normalement est gérée par le politique et l'armée (par les opérations d'information et d'influence «InfoOps»: dont dépend la conduite de la cyber-guerre défensive et offensive).

En conclusion, deux problèmes sont récurrents pour les 4 axes de cyber-attaques:

- l'identification de l'attaquant; *(comment tracer le/les criminels ?)*
- l'organisation de la défense; *(comment se protéger et l'empêcher d'agir ?).*

Que faire ?

La meilleure façon de lutter contre les cyber-attaques est d'anticiper et se préserver. Il faut unir les forces, informer, se protéger, identifier, dénoncer, etc.

Anticiper :

Pour les entreprises et l'économie, il faut de se former dans le domaine de l'intelligence économique et travailler le plus vite possible avec les services judiciaires de la police (banques, loteries, sport,...) dès le premier soupçon d'être confronté à des cyber-criminels.

Pour la lutte contre le cyber-terrorisme, il faut aussi se former dans le domaine de l'intelligence économique et travailler avec les services judiciaires de la police, d'Interpol, de la Sécurité d'Etat (pour les entreprises de transport, d'énergie, de télécommunication, de la santé et des organismes de l'Etat).

Pour se préserver d'une cyber-guerre il faut se former dans le domaine de l'intelligence économique afin de bien comprendre les différences entre les attaques économiques et les attaques ciblées contre l'Etat. Puis, il faut réunir les forces, c'est-à-dire travailler conjointement avec les services judiciaires de la police, d'Interpol, de la Sécurité d'Etat, le politique et l'armée (par les opérations d'information et d'influence: INFOOPS dont dépend la conduite de la cyber-guerre défensive et offensive): Etat, Armée, Entreprises de transport, d'énergie, de télécommunication, de la santé, etc.

Unir les forces et informer :

Pour l'économie, c'est-à-dire les entreprises :

Pour protéger efficacement nos entreprises, notre économie et notre savoir, il faut que chaque entreprise de notre pays mette en place une structure d'intelligence économique en son sein (selon la norme AFNOR XP X50-053 par exemple) avec un responsable de son fonctionnement. C'est au Conseil d'administration de l'entreprise qu'incombe la responsabilité d'en donner l'ordre et de la contrôler.

Pour l'Etat, c'est-à-dire la Confédération

Pour protéger efficacement la Confédération, il faut créer au sein de la Chancellerie fédérale une «cellule intelligence» regroupant l'intelligence économique et l'InfoOps (conduite des opérations d'information et d'influence) chapeautant deux sous-cellules distinctes:

- La première sous-cellule s'occuperait de la sensibilisation des entreprises suisses à l'intelligence économique ainsi que l'encouragement aux Hautes Ecoles pour la création de formations en intelligence économique au profit de l'économie;
- La deuxième sous-cellule disposerait d'une «intelligence transversale» aux sept départements fédéraux dans le domaine de la conduite des opérations d'information et d'influence comprenant l'ensemble des actions de cyber-défense. Cette dernière serait étroitement liée au commandement de l'Armée.

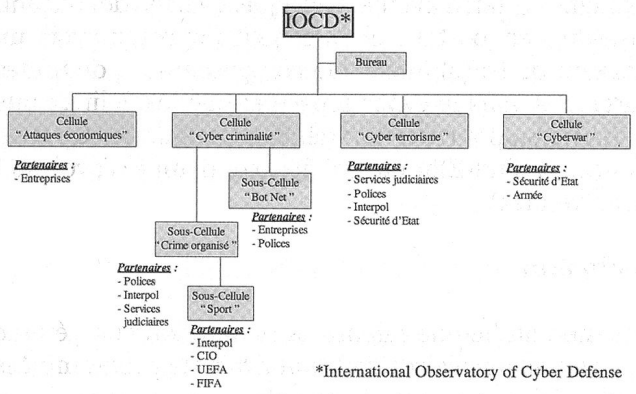
Pour unir les forces et offrir une vision philanthropique internationale de la Suisse :

La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI réunissant des partenaires qui travaillent dans le domaine de la sécurité des systèmes informatiques et de l'Internet ainsi que dans celui de la protection des infrastructures nationales et vitales ne suffisent pas !

La Confédération suisse, en tant que pays neutre et offreur de « bons offices » devrait disposer d'un « Observatoire mondial de la Cyber-défense » bénéficiant :
- d'un partenariat et d'une reconnaissance de l'OSCE, d'Interpol, des Etats ;
- d'une légitimité quant à sa neutralité ;
- d'une légitimité technologique ;
- d'une légitimité juridique ;
- d'une légitimité militaire.

Pour la Suisse, il serait très facile de créer un tel observatoire en partenariat avec les hautes écoles de notre pays (EPFZ, EPFL, HES), les polices cantonales, Interpol, l'OSCE, l'Office fédéral de l'informatique, etc. et offrir ainsi nos bons offices aux autres états dans le monde par :
- des compétences internationalement reconnues ;
- une légitimité quant à sa neutralité, ses technologies, le juridique, le militaire, etc. ;
- un centre technologique d'investigation ;
- un centre de formation (en intelligence économique et militaire).

Cet observatoire pourrait être structuré de la manière suivante :



En cas « d'appel au secours » d'un Etat venant de se faire « cyber-attaquer », l'observatoire pourrait proposer ses services (bons offices), analyser les faits et dresser pour l'avenir une liste de recommandations et de correctifs pour l'avenir à l'Etat concerné.

Se protéger :

Que font les différentes nations dans le monde en matière de cyber-défense ?

Par exemple, les USA accordent une très grande importance à ce domaine. Un « Cyber Commande » a été créé en 2010 et est responsable pour la conduite des opérations offensives dans le cyber-espace ainsi que de défendre les systèmes militaires. Il dispose d'une antenne dans chaque service : USAF, US Army, Navy, Marines. Le NSA joue également un rôle clé avec des compétences au niveau stratégique. Le budget est pour cette année de 2.3 Mia d'US$.

En Chine, le maintien du secret empêche une vision claire et rend difficile l'appréciation de la situation. Cependant, l'inscription du plan quinquennal 2011-2015 du parti au pouvoir démontre, qu'en matière de guerre électronique et d'espionnage cybernétique, l'Etat y porte une très grande priorité et qu'il lui donne des moyens importants. L'Etat collabore étroitement avec des groupes de hackers et des firmes privées leur donnant en échange accès à leurs résultats R&D. La Chine tente de rattraper son retard par rapport à ses moyens militaires conventionnels face aux USA par une supériorité dans le domaine de la guerre de l'information. Elle tente par ce biais un usage politique du cyber-espace.

La Russie ne dit rien sur ses intentions dans ce domaine. En termes de défense, l'armée semble fortement orientée sur des mesures d'opérations de sécurité et des procédures héritées de la guerre froide. En termes de cyber-attaques, la Russie paraît très active, L'armée et les services de renseignement sembleraient bien dotés et soutiendraient financièrement de nombreuses initiatives pour le développement de compétences chez les jeunes.

En termes de défense, Israël est confronté à des attaques quotidiennes provenant notamment de l'Iran et prend cette menace très au sérieux. Ce mois de juin, Israël a annoncer la création d'une unité de cyber-défense, car jusqu'à maintenant l'armée et le gouvernement s'était concentrés sur le développement de solutions offensives. Ses moyens sont bien structurés. Sur le plan civil, une branche pour la sécurité des infrastructures existe et sur le plan militaire, trois branches : sécurité interne, protection contre les attaques extérieures et défense nationale sont sur pieds. Il n'existe toutefois pas d'autorité générale chapeautant l'ensemble.

L'OTAN dispose d'un CERT et du « *NCIRC Technical Centre* » bases en Estonie : le NATO Computer Incident Response Capability - Technical Centre (NCIRC TC) et le NATO Computer Incident Response Capability (NCIRC). Ce centre de compétences supporte la communauté des armées de l'OTAN, mais chaque pays garde sa propre souveraineté sur la protection de ses systèmes d'information militaires.

En conclusion, nous constatons qu'aucun pays ne dispose actuellement d'une solution d'ensemble, d'une coordination et d'une entité de responsabilité suprême. Chaque pays dépense des sommes considérables en matière de cyber-guerre, plus dans des moyens offensifs que défensifs. Tous les pays, même la Russie et la Chine, font appel à des partenariats privés publics (PPP) pour le développement des technologies dans le domaine du cyber-espace et qu'actuellement aucun Etat ne dispose d'une vraie solution de cyber-défense.

Parmi les plus grands défis pour toute armée au monde, le pouvoir d'évoluer dans un milieu informationnel sûr, exempt de toute menace d'écoute, de fuite, d'intrusion, de dénis de services, et autres cyber attaques – sans pour autant limiter sa liberté d'action - est l'enjeu majeur. Les solutions de protection classiques sont souvent rédhibitoires en termes d'utilisation (bridage des applications MS-Office, ralentissements inhérents au cryptage fort (à l'encryptage), passerelles complexes sur le monde extérieur, etc.) ne sont donc pas viables dans un environnement opérationnel exigeant et mouvant.

Ce défi est d'autant plus grand que les armes cybernétiques sont désormais accessibles à tous, et prolifèrent sans contrôle. Nulle barrière technologique, financière ou légale n'en entrave efficacement la multiplication. Le conflit dans le cyberespace est dissymétrique en faveur de l'attaquant. Celui-ci peut facilement mener une agression en profitant des dernières évolutions technologiques, alors que le défenseur doit en permanence mettre l'ensemble de ses dispositifs de sécurité au niveau de la menace.

L'enjeu est « simple » : *il s'agit de se protéger contre les effets des « Cyber attaques » quelles qu'elles soient, afin de rétablir la symétrie*

Lorsqu'on peut rétablir la symétrie dans la cyber-guerre, on peut la gagner ensuite avec d'autres moyens plus conventionnels sur le terrain, sur la base de la guerre informationnelle: en défendant mes « tuyaux » et attaquant ceux de l'adversaire pour protéger notre processus décisionnel et détruire le sien.

Pour se prémunir contre les cyber-attaques, il faut mettre en place un système de défense efficace basé sur l'anticipation et l'intelligence collective ! Cette solution existe et elle est suisse. La solution MDTS² (Miltary Data Traffic Security Service) proposé par Satorys à Genève, sécurise totalement un réseau militaire contre toutes les cyber-attaques connues et à venir, c'est-à-dire tous les postes de travail, les téléphones, les smartphones et les systèmes embarqués.

Cette solution est unique au monde. Elle se base sur une approche complètement nouvelle, l'analyse comportementale intelligente de tous les flux de données et non sur la reconnaissance de signatures, comme la plupart des solutions disponibles sur le marché. Elle est aussi la première à travailler sur le principe de la pro-activité et de l'intelligence collective. Elle offre les avantages suivants:

- analyse comportementale intelligente de tous les flux de données;
- pas de concentration sur un scénario de risque étroit;
- aucun logiciel est chargé ou déployé sur les stations clients;
- utilisation des logiciels « standards » non bridés tel que MS-Office;
- pas besoin de cryptage dans l'environnement contrôlé;
- avertissement en temps réel d'un problème quelconque;
- minimum de formation nécessaire pour les superviseurs MDTS²;
- mise à disposition d'une intelligence collective;
- pas de formation spécifique pour les utilisateurs;
- Pop-Up de mise en garde avec instructions nécessaires clairement données;
- détection automatique de problèmes;
- mise à jour en temps réel;
- protection totale contre les types de cyber-attaques actuelles et futures.

Avec cette solution, tous les problèmes énoncés dans la presse (Stuxnet, Loockeed Martin, etc.) auraient pu être évités! Stuxnet n'a aucun effet. L'armée qui utiliserait cette solution serait efficacement protégée et pourrait être connectée à l'Internet, pourrait supprimer les anti-virus et, suivant l'environnement, pourrait supprimer l'encryption! Et de plus la téléphonie ainsi que les notebooks et les smartphones utilisés seraient totalement protégés. Les partenaires, c'est-à-dire les autres armées, partie prenantes d'une opération (exemple: l'OTAN en Afghanistan) tout comme les ONGs peuvent s'interconnecter sans soucis de fuite d'information ou de risque de contamination entre réseaux.

Pour les infrastructures critiques du Pays, mais aussi pour les opérateurs, les entreprises et les banques du secteur de l'économie privée, la solution similaire en version civile existe. Elle garantie la même approche et le même niveau de sécurité.

Identifier, dénoncer:

Dernier point très important: informer de façon systématique et dénoncer de manière collective et structurée. Il ne faut pas, sous prétextes de la honte, du maintien de la confidentialité ou tous autres arguments, vouloir passer sous silence le fait d'avoir été attaqué. C'est en dénonçant, c'est-à-dire en portant plainte qu'il pourra y avoir un maximum de traçabilité et de compréhension de toutes les attaques dans le cyber-espace et que les délinquants pourront être poursuivis et déferrés en justice. C'est en dénonçant qu'un Etat pourra être condamné d'avoir nui à un autre Etat.

Conclusion

Si Stuxnet, au lieu de ralentir la production énergétique des centrales nucléaires de l'Iran avait été programmées pour les faire exploser, le monde aurait appris, à ses dépends, ce qu'auraient pu être les effets létaux de la « guerre virtuelle » ou du cyber-espace.

Nous devons « civiliser » le monde virtuel qu'est l'espace cybernétique et en faire un espace respectant les lois connues dans le monde réel. Pour y parvenir, les chefs d'Etats, les militaires, les juristes et l'économie doivent réfléchir ensemble et définir ensemble les règles ainsi que les moyens de protection. Si toutes ces protections et ces lois sont mises rapidement en place, même si la guerre cybernétique a déjà commencé, elle n'aura finalement jamais de concrétisation.

S. A.