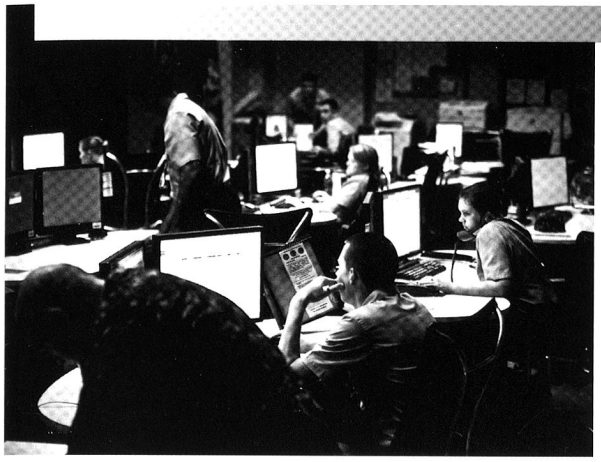
Vers une Cyber Défense de la Suisse



L'US Cyber Command.

Guerre de l'information

Vers une Cyber Défense de la Suisse

Col EMG Gérald Vernez, maj Ricardo Sibilia

Directeur suppléant du projet Cyber Defense, DDPS, Secrétariat général. Chef de la cyber analyse, DDPS, Base de l'aide au commandement

Les menaces cybernétiques sont pour la Suisse un défi sécuritaire important dont les contours flous et dynamiques réclament rapidement une solution à l'échelle nationale. Le Conseil fédéral a ordonné en décembre 2010 que soit établie d'ici à la fin 2011 une stratégie pour la Cyber Défense. Cet article résume les premiers résultats du groupe de travail.

Avant-propos

On ne trouve pas d'exemple comparable dans l'histoire, où autant de développements technologiques ont été accomplis et assimilés en aussi peu de temps. La « révolution de l'information » de ces 25 dernières années représente une avancée considérable et un bénéfice incalculable pour la société. Mais la médaille comporte malheureusement un revers. En effet, en raison de notre dépendance désormais totale des technologies de l'information et de la communication (TIC), leur dysfonctionnement a le potentiel d'entraîner des conséquences immédiates et sévères pour notre société. L'éventualité de telles perturbations découle des nombreuses imperfections de ces systèmes qui peuvent être exploitées par des parties en conflits, des criminels et des individus mal intentionnés qui ont compris l'usage qu'ils peuvent en faire.

En utilisant les forces et les faiblesses des TIC, ces acteurs ont en effet aujourd'hui la possibilité de frapper n'importe qui, depuis n'importe où, n'importe quand, tout en restant indétectables et donc impunis. Les attaques informationnelles via le cyberspace permettent la surprise et la déception parfaites. Des effets majeurs peuvent être atteints avec de faibles investissements, alors que le défenseur doit faire des efforts importants sans garantie de succès. La dissymétrie de ces rôles est totale. Et il faut ajouter la complexité croissante du « système de systèmes » qui se met en place et dont nous perdons graduellement la vue d'ensemble et dont les limites s'estompent, ce qui rend sa défense encore plus difficile. La probabilité que dans toute cette complexité des pannes se déclenchent sans main criminelle pour les provoquer augmente fortement, comme nous l'a rappelé l'exemple de Fukushima et ses crises emboîtées.

Avec son très haut standard de développement, la Suisse tire tous les avantages possibles des progrès offerts par les TIC; elle en est même un important moteur. Mais notre degré de dépendance aux TIC fait que nous sommes également supérieurement exposés. Il est « midi moins cinq » pour évaluer honnêtement les risques et en tirer enfin les conséquences, car bien qu'avancés en comparaison internationale, nous n'avons de loin pas fait tout ce qui devrait l'être. Lors de sa séance du 10 décembre 2010, le Conseil fédéral a reconnu qu'il est urgent d'agir et ordonné l'établissement d'une Stratégie Nationale de Cyber Défense d'ici à la fin 2011.

L'élaboration de cette stratégie doit répondre à de nombreux défis allant bien au-delà des simples considérants technologiques et informatiques. En effet, il s'agit d'apporter une réponse à des risques complexes de nature civile et militaire, privée et publique, nationale et internationale dans une complète « intransparence. » Comment affirmer la souveraineté de l'Etat sans menacer les intérêts privés et de la personne? Comment répondre à une question a priori technique, mais dont les conséquences relèvent à l'évidence de la politique de sécurité ? Quelle est notre place et notre responsabilité dans la mise au point d'une solution internationale? Quel doit être notre degré d'ambition? Ce qui s'avère d'ores et déjà comme essentiel, c'est de considérer ce thème comme relevant de la politique de sécurité dans lequel l'Etat et la société doivent investir rapidement les ressources nécessaires.

La stratégie devra apporter une réponse à un problème dont on sait qu'il aura d'autres caractéristiques l'an prochain déjà. Elle devra apporter une réponse d'ensemble à un réseau de problèmes complexes alors que les détails ne seront établis qu'après une longue cartographie restant à réaliser. Le provisoire risque donc d'être une des nos rares constantes! Notre posture actuelle, essentiellement réactive et liée aux événements devra passer à une posture proactive visant à éviter autant que possible la surprise. Le schéma traditionnel où l'Etat apporte seul toutes les solutions devra être remplacé par une vision en réseau regroupant tous les acteurs, individus, entreprises et l'Etat. Les solutions et contre-mesures technologiques

joueront un rôle important, mais ce ne sera qu'une partie de la solution. Réduire la cyber défense à un « machin vite fait dans la sécurité informatique », ou ne pas y consacrer les moyens nécessaires, serait se tromper lourdement et s'assurer un prochain réveil vraiment douloureux !

Caractérisation générale de la cyber-menace

Le niveau de pénétration croissant des TIC dans nos sociétés permettent à des dysfonctionnements de se propager à toute la société. Du fait de leur complexité, de la nature des technologies employées, de la manière dont elles sont configurées, du nombre élevé de fautes (voulues ou non) qui se cachent dans les centaines de milliards de lignes de codes qui régissent aujourd'hui notre vie, les TIC sont par nature imparfaites. La multitude de failles qu'elles comportent peuvent, dès lors qu'elles ont été identifiées, servir des dessins belliqueux. N'importe qui, de l'employé frustré à l'Etat agressif en passant par la criminalité organisée et le terrorisme peut en tirer avantage. Et en plus de la main ennemie il convient aussi de considérer les événements accidentels dont les effets sont similaires à ceux d'attaques délibérées.
Prétendre que rien n'a été fait jusqu'ici serait injuste à l'adresse de ceux qui se battent sur ce front depuis plusieurs années et qui ont mis sur pieds un dispositif que bien des pays nous envient. Mais ce dispositif ne peut pas réaliser toutes les tâches requises car il est basé sur le volontariat, ne couvre pas tous les domaines, ne dispose pas d'une conduite permanente et n'a aucune capacité à durer ou à monter en puissance. Il n'a pas démérité, mais le potentiel de la menace est désormais tel, que l'on ne peut plus admettre ces faiblesses. Ce dispositif a été prévu pour des actes criminels qui, bien qu'importants en nombre et en dommages, se concentrent sur les biens et intérêts privés. Avec une menace qui évolue désormais vers une dimension stratégique où les intérêts de l'ensemble de la société et donc de l'Etat sont en jeux, ce dispositif ne suffit plus.
Même si l'usage de la dimension informationnelle en tant que moyen de politique de puissance reste cantonné à l'espionnage et dans des exemples controversés (Estonie, Géorgie, Iran), ce potentiel ne peut en aucun cas être ignoré. Tous les indicateurs montrent en effet que les moyens, le savoir-faire et la volonté d'en faire un usage comme arme à part entière progressent à grand pas dans de nombreux pays. En Suisse, il a fallu l'attaque contre le Département des affaires étrangères et celle contre les installations d'enrichissement d'uranium de l'Iran (cas STUXNET) pour que nous en admettions l'inéluctable développement et ses conséquences potentielles pour notre Pays.

Qu'est-ce que le cyberespace?

La complexité des TIC ainsi que leurs interactions avec le milieu physique et les personnes implique que l'on ne peut plus voir le cyberespace comme un simple amoncellement d'appareils. Dans le cadre du projet Cyber Defense, nous avons adopté la définition suivante: le cyberspace est l'environnement opérationnel dans lequel des données sont saisies, conservées, transmises, modifiées, organisées, codées, représentées et transposées en actions physiques.
La première question qui vient à l'esprit est : mais qui est responsable de ce cyberespace? Il n'y a pas de réponse simple à cette question. L'Etat a de toute évidence pour tâche d'amener l'ensemble des acteurs nationaux à des solutions communes pour utiliser et sécuriser cet espace dans le cadre de sa souveraineté, mais celle-ci devra être précisée. L'Etat devra aussi coordonner ses effort avec les autres Etats dont les intérêts sont souvent divergents et alors qu'il y a absence d'une autorité internationale capable et désireuse d'organiser et d'imposer un point de vue global.

Conditions d'une agression cybernétique

Afin qu'une agression puisse avoir lieu dans le cyberespace, trois conditions sont requises.

- Le système pris pour cible doit disposer d'une ou de plusieurs vulnérabilités, dont l'exploitation pourrait avoir des conséquences importantes ;
- Il faut que l'existence de ces vulnérabilités soit connue ou supposée, savoir comment les trouver et en tirer avantage;
- L'acteur qui connaît l'existence de ces failles et les conséquences de leur exploitation doit avoir un motif pour passer à l'acte.

C'est ici la traditionnelle trilogie POUVOIR – SAVOIR – VOULOIR, une attaque est obligatoirement la combinaison de ces trois éléments et seuls les actes accidentels dérogent à cette règle.

Pas de sécurité à 100%

Du côté des défenseurs, il ne s'agit pas de trouver une faille et de la corriger, mais de toutes les trouver et de toutes les corriger ce qui est non seulement ruineux mais aussi impossible à réaliser, alors qu'il suffit à l'attaquant de trouver la seule faille oubliée par les défenseurs pour atteindre ses objectifs. Il y a donc une dissymétrie totale entre attaque et défense. Certaines failles sont par ailleurs connues que d'un petit nombre d'agresseurs, on parle alors de « 0-day Vulnerabilities » , qui les vendent pour quelques dizaines de milliers de dollars. L'attaque menée par ce biais est alors indétectable et imparable. Dans le cas de STUXNET ce sont quatre failles de ce type qui ont été utilisées. Il y a aussi les failles laissées illégalement par des développeurs qui souhaitent conserver des « portes dérobées » pour divers motifs, mais il arrive aussi que des accès soient réclamés par des Etats qui ont besoin d'une entrée discrète pour leurs services de renseignements.
Et si un logiciel est parfait, sans faille de sécurité ni connexion à Internet est-il pour autant sûr ? Non, car il se trouvera toujours un *insider* corruptible, négligeant ou malveillant qui introduira directement un ver ou un virus avec un stick USB, comme cela a été le cas pour STUXNET et CONFICKER, ou qui réussira à extraire des données comme en ont récemment souffert quelques banques.
Les TIC ne peuvent pas être sécurisées à 100%. Si une solution de sécurité s'avère « incassable », ce caractère ne dure jamais bien longtemps et se vanter sur la Toile d'avoir créé l'arme absolue contre les hackers revient à les provoquer. Rares sont les sociétés qui ont tenté une telle stratégie commerciale : la dernière à l'avoir fait a

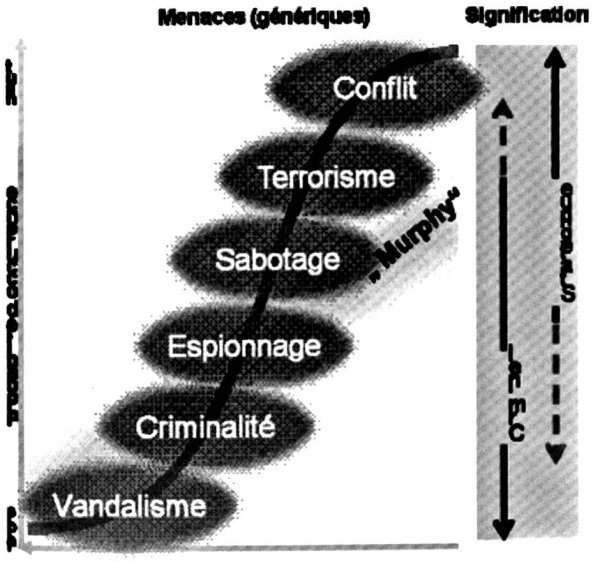
déposé le bilan trois semaines après! Le « combat » entre attaquants et défenseurs est à l'avantage du premier car il bénéficie de l'effet de l'initiative alors que le second s'épuise à courir derrière les failles et à expliquer aux concepteurs et aux responsables financiers réfractaires que les fonctionnalités et le confort doivent passer après la sécurité, surtout dans des environnements exposés.

Développement de la menace

Les notions de cyberespace et de menaces cybernétiques sont apparues dans les années 80 et n'ont cessé de prendre de l'ampleur avec le développement fulgurant des TIC. Le premier ver informatique a été créé en 1971 et s'est répandu sur ARPANET, l'ancêtre d'Internet. Le premier ordinateur digital appelé COLOSSUS date de 1943 et servait à l'analyse à Bletchley-Parc de la cryptographie des messages stratégiques allemands du code Lorenz. Depuis la fin des années 90, les logiciels malveillants n'ont cessé d'être développés. Au début il s'agissait d'un jeu pour amateurs, même si parfois des dommages importants en ont résulté comme avec le virus ILOVEYOU. Aujourd'hui ce domaine s'est professionnalisé et il est permanent et global. Si on admet communément que la cyber criminalité trouve son origine dans le pays de l'ex-URSS et en Chine, plus aucun pays n'est épargné. De 100 nouveaux virus par jour en 2007, nous sommes passés à 3000 en 2010. CONFICKER et STUXNET montrent qu'une étape à été franchie, car même des systèmes physiquement séparés d'Internet peuvent désormais être attaqués avec précision. Certains auteurs parlent même de « missiles de croisière informationnels. »

Les attaques cybernétiques vont prendre inéluctablement de l'ampleur car:

- le nombre de failles et d'imperfections qui peuvent être atteintes grâce à la mise en réseau, leur criticalité et les moyens d'attaque disponibles pour quelques dollars sur Internet, augmentent sans cesse;
- le savoir-faire pour réaliser des attaques est toujours plus bas et plus facilement accessible, ce qui le met à la portée d'un nombre croissant d'agresseurs;
- le nombre d'acteurs prêts à passer à l'acte ne cesse de croître en raison des avantages de ce type d'attaque (simplicité, efficacité, impunité, rendement / gain élevé, effet de surprise, déception, indépendance géographique et temporelle).



Les attaques contre les infrastructures SCADA (Supervisory Control And Data Acquisition ; informatique de pilotage des processus industriels), contre la téléphonie mobile qui va incorporer le trafic des paiements, contre les smart grids destinés à réguler la distribution d'électricité, contre les activités de l'Etat (e-democracy, e-voting, etc.), contre les forces de sécurité, contre l'identité des personnes, etc. vont donc se multiplier. Comme indiqué plus haut, dès que la trilogie pouvoir – savoir – vouloir est satisfaite, tout peut arriver.

Formes de la menace

Les menaces cybernétiques ne peuvent pas être réduites à un problème d'informatique. Nous devons avant tout comprendre les acteurs et leurs motivations. Pour y mettre bon ordre, une classification a été établie sur une base phénoménologique. Elle n'est pas une fin en soi et nous sommes conscients de ses limites, mais elle permet d'ordonner plus facilement les réflexions en cours.

Vandalisme : Lorsque des millions d'internautes utilisent le cyberespace pour se mesurer, se défouler ou s'engager massivement au profit d'une cause et infliger des « cyber-punitions » comme ce fut le cas en Estonie en 2007, le problème clé est le nombre d'agresseurs. Ces attaques se caractérisent par leur hétérogénéité, leur durée et leurs effets peuvent aller de simples perturbations jusqu'à des destructions. Dans ce cas, la justice peut faire quelques exemples, mais la poursuite de centaines de milliers d'actes répréhensibles dont les auteurs sont difficiles à identifier est impossible.

Criminalité : Le profit est ici le moteur et de nombreux gangs internationaux se développent. Professionnels, ils disposent de moyens techniques, financiers et humains parfois supérieurs aux Etats. Ils sont rapides, flexibles et maîtrisent les subtilités du droit et commettent tous les délits possibles (vols, chantages, falsification, etc.) pour eux-mêmes, mais aussi pour des commanditaires étatiques ou économiques. Au contraire du vandale qui veut voir ses « tags » sur les murs, ces criminels vont tout faire pour rester indétectables afin que leur opération dure et soit le plus rentable possible.

Espionnage : Pour satisfaire des motivations politiques ou pécuniaires, les TIC permettent un pillage illimité du savoir. La liste des acteurs comprend des Etats et leurs services de renseignements, mais aussi des privés agissant au profit de tiers, ou des industriels désireux de contrôler ou d'affaiblir la concurrence. Comme pour la criminalité, ces actes restent le plus souvent non détectés et lorsqu'ils le sont, ils ne peuvent que rarement être attribués.

Sabotage : Lorsque pour des raisons politiques ou militaires il faut frapper avec précision des cibles pour paralyser l'adversaire, l'aveugler, le tromper, etc. les TIC permettent des résultats rapides, discrets et bon marchés, sans devoir exposer la vie des opérateurs. Toutes les

infrastructures critiques peuvent être prises pour cible pour infliger des dommages économiques, appuyer des actions militaires ou jeter le discrédit sur la victime qui n'a pas su défendre ses intérêts ou qui se retrouve l'auteur involontaire d'une pollution majeure. De telles actions sont à la portée d'acteurs isolés.

Terrorisme : Pour l'instant, les experts admettent que les terroristes utilisent encore Internet et les TIC essentiellement pour recruter leurs membres, les instruire, faire de la propagande et piloter leurs opérations, mais qu'ils ne les prennent pas encore pour cible. Mais il est aussi admis que la violence à caractère politique va de plus en plus s'exprimer dans des actes conduits par et contre le cyberespace. Il y a des millions de jeunes bien formés et désœuvrés qui pourraient aussi voir là un moyen de se faire entendre.

Conflit : L'arme informationnelle prend une place croissante dans les arsenaux militaires. Ce moyen pourrait supplanter les effecteurs cinétiques de la guerre traditionnelle dont la létalité est de moins en moins admise. En conduisant ses opérations dans le cyberespace un Etat pourrait surprendre et défaire un adversaire sans devoir tirer un coup de feu. Le seul obstacle à un tel scénario est l'immensité de la tâche, mais dès lors que la faisabilité des éléments constitutifs d'une telle attaque est établie, il n'y a qu'un pas jusqu'à sa réalisation. Ce scénario doit donc être pris au sérieux. Le laisser de côté au motif que l'on n'en a pas encore vu serait irresponsable. Les attaques contre la Serbie en 1999, l'Irak en 2003, le Hezbollah en 2006 au Liban, l'Estonie en 2007 et la Géorgie en 2008 démontrent que la volonté et le savoir-faire sont là. Il ne reste qu'à patiemment dresser la liste des failles et à préparer le terrain. Même sans évoquer une « guerre généralisée dans le cyberespace », ces exemples montrent déjà que les capacités militaires sont des cibles prioritaires ; équiper une armée de TIC sans consacrer les efforts nécessaires à leur sécurisation est donc du suicide préprogrammé. Et si les armées ne disposent pas des compétences requises pour de telles attaques ou ne souhaitent pas être identifiables comme agresseur dans le cyberespace, de nombreuses sociétés criminelles se bousculeront pour prendre des mandats.

Accidents : comme déjà développé plus haut, il s'agit aussi de considérer toutes les perturbations dont les effets sont similaires à ceux d'actions intentionnelles mais qui trouvent leur origine dans des erreurs de conception, la négligence, ou une complexité qui n'est plus maîtrisée. On pourrait aussi parler de « Murphy », ce redoutable adversaire qui est toujours là où il ne faut pas... !

Le problème pour l'Etat est de savoir quand une attaque est de nature criminelle et quand elle devient stratégique afin de prendre les bonnes décisions. Il s'agit donc de disposer de procédures permettant d'assurer une réponse synchronisée de nos instruments de politique de sécurité, des exploitants de nos infrastructures critiques et de nos partenaires internationaux. Il faut assurer une gestion continue allant des bagatelles quotidiennes jusqu'aux situations de conflit entre Etats. Il faut apprendre à gérer les basculements qui peuvent être induits par des masses de personnes ou de systèmes entrant en action. Des Etats jugés encore stables en janvier ont en effet été secoués et transformés en quelques semaines par des activistes dépassant les forces de sécurité partout avec YouTube, Twitter et Facebook. Même s'il est évident que la Suisse ne va pas s'engager sur un tel terrain, nous devons comprendre de tels mécanismes.

Signification pour l'armée

Les intersections quotidiennes entre sphères privée et sphère professionnelle à travers les ordinateurs, smartphones et stick USB représentent pour l'armée un défi ; une nouvelle culture de sécurité pour palier aux erreurs quotidiennes que nous commettons tous et qui peuvent être exploitées par des intentions malveillantes est nécessaire. Si on y ajoute l'hétérogénéité des systèmes, des normes et de leur mise en œuvre, ainsi que des comportements non adaptés face à de tels problèmes, voilà autant de points de faiblesse qu'un agresseur peut mettre à profit pour empêcher notre armée d'accomplir sa mission.
Face à une menace qui peut avoir des effets globaux et immédiats sans aucun avertissement, l'armée va rester encore longtemps le seul moyen disposant de la masse suffisante pour apporter aide et sécurité à l'échelle du Pays. La condition est bien sûr qu'elle soit disponible et efficace rapidement dans n'importe quelle situation. La multiplication des tâches qui découlent des scénarii d'attaques cybernétiques majeures plaide donc pour une armée nombreuse, équipée, entraînée et rapidement mobilisable en toute circonstance pour des tâches de surveillance, de stabilisation et d'aide. Une telle situation plaide aussi pour un degré de sophistication technique permettant de répondre sereinement aux questions suivantes : sommes-nous en mesure d'acquérir des équipements high tech en grand nombre, de les déployer, de les engager dans un environnement informationnel dégradé, de les entretenir, de les remplacer et de les protéger en opération? Les auteurs de ces lignes ont leur petite idée là-dessus... Et il convient de ne pas oublier la pénurie croissante de personnel qualifié dont se plaint l'économie et qui commence aussi à entraîner des conséquences désagréables pour l'armée.

Conditions cadre d'une solution

Le délai rapproché imposé par le Conseil fédéral est sage. Si tous les observateurs ont salué cette décision, beaucoup craignent encore que cela soit un « exercice alibi ». Mais les acteurs de ce dossier sont conscients que la Suisse n'a pas le droit d'échouer, ni de repousser une fois encore l'opérationnalisation d'une solution pour faire face à une menace devenue quotidienne. On ne peut pas non plus se permettre d'attendre une solution parfaite. Il s'agit au contraire de déclencher sans tarder la mise en œuvre d'un dispositif qui sera ensuite constamment amélioré. Rome non plus ne s'est pas faite en un jour! La tendance de se ruer sur la planche à dessin pour élaborer des organigrammes est un danger commun à tous les projets. Pour s'en prémunir, onze thèses ont été développées

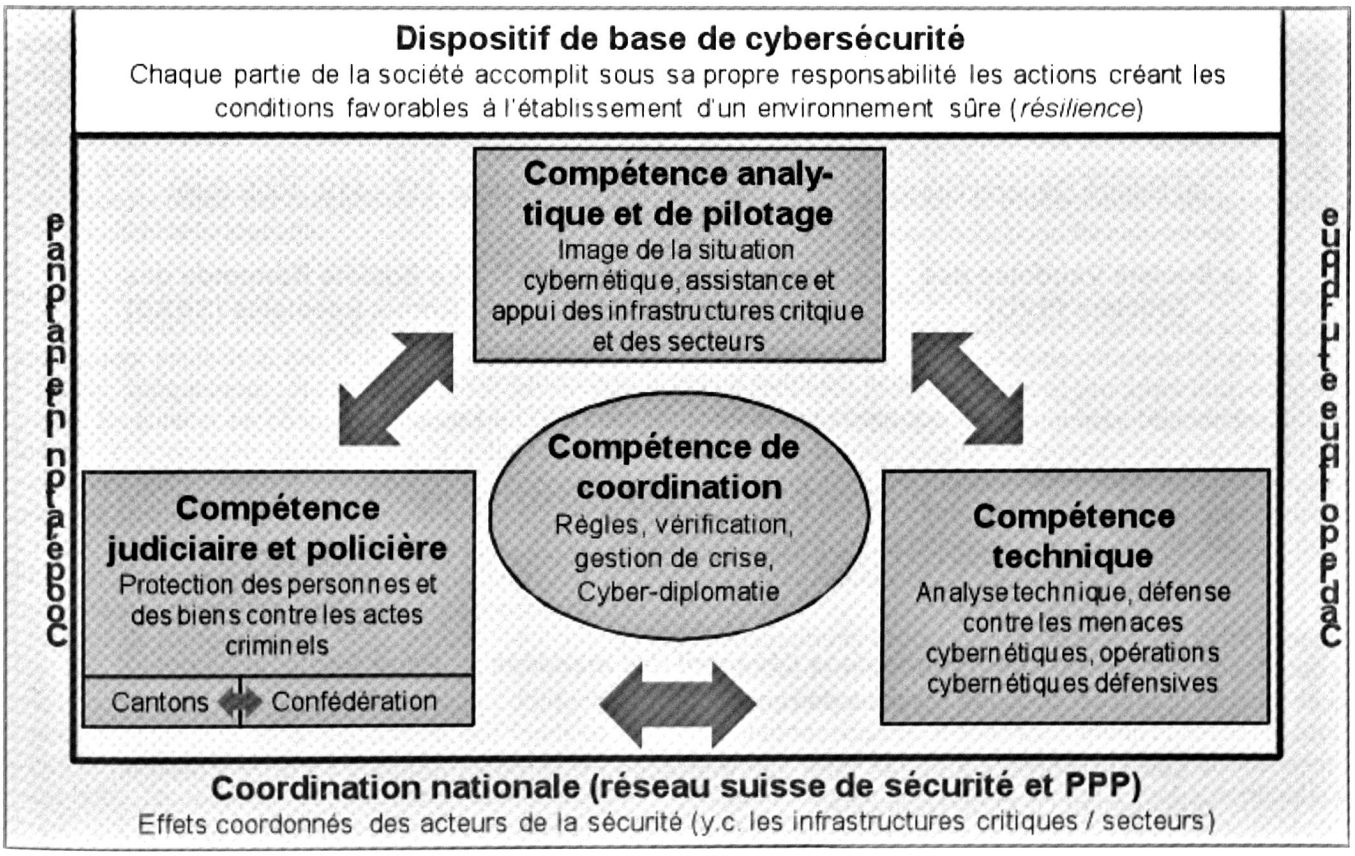
comme autant de critères permettant de vérifier que la direction est bonne. Elles stipulent qu'il faut :

- une approche « top – down » (vision, stratégie, processus, moyens);
- un cadre politique et légal clair ;
- augmenter la résistance de notre société, sa capacité à gérer les crises et à récupérer après celles-ci ;
- s'assurer que les acteurs disposent d'un vocabulaire commun ;
- s'assurer que le dispositif dispose d'une haute disponibilité et réactivité ;
- rendre les individus aptes à évoluer au quotidien malgré les menaces cybernétiques; assurer une conduire de la manœuvre (pas d'auto-gestion);
- mettre les infrastructures critiques et l'économie au centre de notre dispositif ;
- établir un réseau de coopérations nationales et internationales avec des partenaires choisis ;
- passer à une posture proactive et investir dans la recherche et dans la prospective ;
- comprendre le principe de « responsabilité collatérale » (en quoi mon comportement peut-il entraîner des conséquences chez mon voisin / autrui ?).

la Constitution fédérale. Si certains détails de l'analyse et des solutions envisagées ne peuvent pas être divulgués sur la place publique, la discussion est conduite de manière transparente avec de nombreux partenaires et le projet cyber défense communique ouvertement ses principaux résultats avec tous les milieux intéressés. Dans l'état actuel des réflexions, le dispositif prévu comprendra les trois éléments principaux de la figure ci-contre, à savoir:

Dispositif de base de cybersécurité : sans ce socle et l'augmentation générale de la résilience de la société suisse qui devrait en résulter, toutes les autres mesures seront vaines. L'absence de ce socle signifierait que le traitement de tous les incidents devrait être attribué à une instance centrale, ce qui serait un non sens opérationnel, légal et financier. Il s'agira de définir quelle entité devra atteindre quel niveau, quel standard sera obligatoire et lequel sera facultatif, étant entendu que plus la criticalité d'un processus ou d'un système est grande, plus son propriétaire devrait être tenu d'appliquer des règles strictes pour en protéger le fonctionnement.

Les compétences : les quatre compétences mentionnées au centre de la figure ci-contre devront appuyer subsidiairement les exploitants des infrastructures critiques et les acteurs du réseau suisse de sécurité lorsque ceux-ci seront dépassés par l'ampleur des



Stratégie nationale de cyber défense

« Nous voulons un dispositif dynamique d'appui et de protection contre les menaces cybernétiques afin de protéger les fonctions vitales dont la Suisse tire sa stabilité, sa prospérité et sa sécurité ». Telle est la vision vers laquelle tend la stratégie, en droite ligne avec l'article 2 de

menaces auxquelles ils seront confrontés ; pour être efficace rapidement, ce dispositif devra être compatible avec le droit en vigueur et ne pas être subordonné à un développement légal (national et international) dont l'issue serait inconnue.

Les conditions cadres : le cadre politique et juridique devra être clair dès le départ afin d'éviter tout blocage.

La collaboration avec les partenaires nationaux (Confédération, cantons, infrastructures critiques et secteurs économiques) permettra d'insérer la cyber défense dans le dispositif de politique de sécurité ; ce sera une des pierres de l'édifice. La coopération internationale avec des partenaires choisis devra en outre nous permettre de disposer d'une plus grande profondeur de champ.
Bien que proche de l'état définitif, ce dispositif est encore générique. Les détails découleront de la discussion du niveau d'ambition qui devra encore être conduite pour déterminer le prix du dispositif et cette étape est prévue pour cet été.

En conclusion

Il a rapidement été établi que la recherche de la perfection et de l'exhaustivité ne contribuerait pas au succès de la stratégie. Une solution partielle rapidement mise en place puis régulièrement améliorée est donc privilégiée. Le consensus s'établi rapidement grâce à une collaboration très ouverte avec les principaux acteurs, en particulier l'administration fédérale et les exploitants des infrastructures les plus critiques, ceux-ci ayant été identifiés par une étude générale des risques au début du projet. Nous avons dû faire des choix et tous les acteurs potentiels ne pourront pas être entendus ni intégrés dans la discussion cette année, mais la méthode retenue et les travaux de longue haleine permettront ultérieurement de considérer tous les intérêts.
La discussion du rôle des différents acteurs de la cyber défense devra encore être conduite, notamment au sujet de l'armée qui va devoir développer une capacité de « mission assurance » ou de sûreté opérationnelle pour protéger ses TIC pour son fonctionnement de base et ses engagements. Un avis de droit de 2009 établit sa légitimité à disposer de capacités pour se protéger contre des attaques cybernétiques et pour dégrader les TIC adverses en cas de conflit. C'est un début, mais là aussi le niveau d'ambition doit encore être établi afin qu'elle dispose d'un éventail opérationnel complet face à des menaces dont l'horizon temporel est la minute et non pas le mois et l'horizon géographique la planète et non pas le Jura.
Le chemin jusqu'à la présentation au Conseil fédéral de la solution recommandée est court et il reste encore beaucoup à faire, mais les progrès réalisés sont encourageants. Ce qui doit être impérativement compris par tous, c'est que la cyber défense n'est pas une option, mais une obligation, qu'il s'agit d'un élément de notre politique de sécurité et que la solution sera à l'image des TIC, un réseau. Et tout cela aura un coût qui devra enfin être assumé.

G.V. & R.S.