Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS

Stratégie nationale de protection de la Suisse contre les cyberrisques

27.06.2012

SOMMAIRE

RÉSUMÉ

Les technologies de l'information et de la communication (TIC) ont modifié fondamentalement l'économie, l'Etat et la société. L'utilisation du cyberespace (p. ex. Internet et les réseaux mobiles) a certes offert beaucoup d'avantages et d'opportunités. Reste que le réseau numérique permet aussi de perturber le fonctionnement des infrastructures utilisant les technologies de l'information et de la communication (infrastructures TIC) ou d'en abuser à des fins hégémoniques, terroristes, d'espionnage ou de criminalité. Les perturbations, les manipulations et les attaques ciblées commises au moyen des réseaux électroniques constituent des risques inhérents à une société de l'information. On peut donc s'attendre à ce que celles-ci se multiplient à l'avenir.

Puisque la protection des infrastructures TIC contre les cyberrisques représente un intérêt majeur pour la Suisse, le Conseil fédéral a ordonné l'élaboration d'une stratégie nationale de protection de la Suisse contre les cyberrisques. Les objectifs stratégiques qu'il poursuit ainsi sont :

- la détection précoce des menaces et des dangers dans le cyberespace,
- l'augmentation de la capacité de résistance des infrastructures critiques,
- la réduction des cyberrisques liés en particulier à la cybercriminalité, au cyberespionnage et au cybersabotage.

La présente stratégie apporte aussi une réponse à diverses interventions parlementaires récentes réclamant des mesures renforcées contre les cyberrisques.

Les conditions de base essentielles pour réduire les cyberrisques sont et restent la responsabilité individuelle, la collaboration au niveau national entre l'économie et les autorités, ainsi que la coopération avec l'étranger. L'échange permanent d'informations doit assurer la transparence et la confiance. Quant à l'Etat, il doit restreindre ses interventions aux cas où l'intérêt public est en jeu ou agir en accord avec le principe de subsidiarité.

Le traitement des cyberrisques doit être perçu comme faisant partie intégrante d'un processus complet d'affaires, de production ou de gestion dans lequel doivent être inclus tous les acteurs, tant au niveau administratif et technique qu'au niveau de la conduite. Pour adopter un comportement infaillible face aux cyberrisques, il ne faut pas perdre de vue que les très nombreuses tâches et responsabilités dévolues aux autorités, à l'économie et à la population laissent des traces dans le cyberespace. La présente stratégie nationale se fonde sur l'idée que chaque unité organisationnelle des milieux politiques, de l'économie et de la société est responsable de reconnaître les conséquences de ses activités dans le cyberespace, d'intégrer les risques qui en découlent dans ses propres processus et de les réduire autant que faire se peut. Les structures décentralisées de l'administration et de l'économie doivent être renforcées pour assumer ces tâches et les ressources et processus existants utilisés de manière cohérente.

Il est nécessaire de réunir en permanence des informations, techniques ou non, pour examiner et évaluer les cyberrisques globalement et permettre la diffusion des résultats de ces analyses.

Un cas de crise se manifeste par une attaque réussie dont les répercussions sont importantes ; il nécessite de la part des acteurs impliqués, y compris des autorités de poursuite pénale, l'application d'une gestion de crise spécifique.

Partant de ce constat, la présente stratégie propose une série de mesures concrètes réparties en sept champs d'action :

Champ d'action 1	**Mesures**	
Identification des risques par la recherche	1	Recherches nécessaires sur les nouveaux risques en lien avec la problématique de la cybernétique
Champ d'action 2	**Mesures**	
Analyse des risques et vulnérabilités	2	Contrôles indépendants des systèmes Analyses des risques dans le but de les réduire en collaboration avec les autorités, les fournisseurs de prestations TIC et les fournisseurs de systèmes
	3	Analyses de la vulnérabilité des infrastructures TIC sous un angle systémique, organisationnel et technique
Champ d'action 3	**Mesures**	
Analyse de la menace	4	Etablissement de l'image et du développement de la situation
	5	Suivi d'incidents dans le but de poursuivre le développement de mesures
	6	Vue d'ensemble des cas et coordination de cas complexes intercantonaux
Champ d'action 4	**Mesures**	
Formation des compétences	7	Création d'une vue d'ensemble des offres en matière de formation des compétences et identifications des lacunes
	8	Comblement des lacunes par des offres en matière de formation des compétences et recours plus fréquent à des offres qualitativement élevées
Champ d'action 5	**Mesures**	
Relations et initiatives internationales	9	Participation active de la Suisse dans le domaine de la gouvernance d'Internet
	10	Coopération au niveau de la politique internationale de sécurité
	11	Coordination des acteurs lors de leur participation à des initiatives et des bonnes pratiques dans le domaine des processus de sécurité et de sûreté
Champ d'action 6	**Mesures**	
Gestion de la continuité et des crises	12	Renforcement et amélioration de la capacité de résistance (résilience) face aux dérangements et événements imprévus
	13	Coordination des activités en premier lieu avec les acteurs directement concernés et appui des processus décisionnels par l'expertise requise
	14	Mesures actives d'identification des agresseurs et des possibilités de porter atteinte à leurs infrastructures en cas de menace spécifique
	15	Elaboration d'un concept pour des procédures et processus de conduite permettant une résolution des problèmes en temps opportun
Champ d'action 7	**Mesures**	
Bases juridiques	16	Vérification des bases juridiques existantes relativement aux mesures et concepts de mise en œuvre et concrétisation prioritaire des adaptations urgentes

Les organes fédéraux responsables, désignés dans la présente stratégie, doivent mettre en œuvre les mesures susmentionnées dans le cadre de leur mission de base d'ici à fin 2017. Les partenaires appartenant aux autorités, à l'économie et à la société doivent être inclus dans ce processus de mise en œuvre. Un organe de coordination est chargé de vérifier la mise en application des mesures et la nécessité de prendre d'autres dispositions pour réduire les risques. Cet organe de coordination devra être créé au sein d'un service de la Confédération.

1 INTRODUCTION

Le réseau numérique mondial a ouvert la voie vers des possibilités insoupçonnées, pour le meilleur, certes, mais aussi pour le pire. L'Etat, l'économie et la société font un large usage des technologies de l'information et de la communication (TIC) et du cyberespace (Internet, réseaux et applications mobiles, affaires électroniques, administration en ligne, pilotage industriel informatisé, etc.). Toutefois, cela implique aussi que notre dépendance et notre vulnérabilité face aux perturbations, manipulations et attaques en tout genre ne cessent de croître. Les possibilités de perturber le fonctionnement des infrastructures TIC ou d'en abuser à des fins terroristes, militaires, d'espionnage ou de criminalité sont tout aussi illimitées que les emplois positifs que l'on peut en faire. On peut partir du principe, au vu de la tendance actuelle, que la mise en réseau se poursuivra à l'avenir et que ces infrastructures deviendront de plus en plus complexes.

La capacité de la Suisse à fonctionner en tant que système global (Etat, économie, transports, approvisionnement énergétique, communication, etc.) dépend d'un nombre sans cesse croissant de systèmes d'information et de communication (ordinateurs et réseaux). Or, cette infrastructure est vulnérable ; des perturbations généralisées ou persistantes ainsi que des attaques dirigées contre elle peuvent porter de graves atteintes aux prestations techniques, économiques et administratives de la Suisse. Ces attaques peuvent avoir des provenances variées et s'appuyer sur des motifs divers : elles peuvent être le fait d'individus, d'activistes poursuivant des buts politiques, d'organisations criminelles recourant à l'escroquerie ou au chantage, d'espions travaillant pour d'autres nations ou d'organisations terroristes qui veulent perturber ou déstabiliser notre Etat et notre société. L'attrait des attaques impliquant les infrastructures d'information et de communication (TIC) ne découle pas seulement du grand nombre de possibilités de détournement, de manipulation ou de dommages qu'elles permettent, mais aussi du fait qu'elles ne requièrent que peu de moyens et que leurs auteurs peuvent rester anonymes.

La protection[1] des infrastructures TIC contre de telles perturbations et agressions est d'un intérêt majeur pour la Suisse. Bien que de nombreuses mesures aient été prises ces dernières années pour réduire les risques[2] dans le cyberespace, il s'avère qu'elles ne suffisent pas à couvrir tous les cas. Du fait qu'une augmentation encore plus importante des perturbations et des attaques contre ces infrastructures (et, au travers de celles-ci, contre d'autres infrastructures) soit envisageable, le Conseil fédéral a chargé, le 10 décembre 2010, le Département fédéral de la défense, de la protection de la population et des sports (DDPS) d'établir une stratégie nationale contre les cyberrisques. Celle-ci doit montrer contre quels risques la Suisse doit se préparer, les moyens dont elle dispose, où se situent les lacunes et comment celles-ci peuvent être le plus efficacement comblées. La présente stratégie nationale de protection de la Suisse contre les cyberrisques est le résultat de ces travaux[3].

---

1 Elle comprend toutes les mesures destinées à protéger les infrastructures TIC contre les intrusions et l'altération de leurs fonctionnalités, hormis la lutte contre la diffusion de contenus illégaux tels que la pornographie à caractère pédophile. Elle s'occupe des aspects techniques, mais ne traite pas des techniques de désinformation et de propagande.

2 Les risques sont définis par le niveau de dommages et la probabilité d'occurrence des menaces et des dangers. Ces deux aspects sont pris en compte dans la présente stratégie.

3 La présente stratégie apporte une réponse à diverses interventions parlementaires récentes réclamant des mesures renforcées contre les cyberrisques : 08.3100 – Motion Burkhalter : Stratégie nationale de lutte contre la criminalité par Internet ; 08.3101 – Postulat Frick : Criminalité informatique. Mieux protéger la Suisse ; 10.3136 – Postulat Recordon : Evaluation de la menace de cyberguerre ; 10.3625 – Motion CPS-CN : Mesures contre la cyberguerre ; 10.3910 – Postulat Groupe libéral-radical : Organe de direction et de coordination pour contrer les cybermenaces ; 10.4102 – Postulat Darbellay : Elaboration d'une stratégie visant à protéger l'infrastructure numérique de la Suisse.

Les cyberrisques présentent de multiples visages ; ils constituent une menace pour l'économie, la société et l'Etat. Une stratégie efficace de protection contre les cyberrisques passe donc par une approche globale et par l'implication de tous les acteurs, privés et publics, notamment les opérateurs d'infrastructures critiques, les fabricants et les utilisateurs. La présente stratégie de protection de la Suisse contre les cyberrisques s'adresse en premier lieu aux organes de la Confédération et a été élaborée avec des représentants de tous les départements, de différents opérateurs d'infrastructures critiques, de fournisseurs de prestations TIC, de fournisseurs de systèmes et des milieux économiques. Elle décrit le rôle dévolu à chaque acteur et l'organisation de leur collaboration pour parvenir à la meilleure protection possible contre les cyberrisques ; elle constitue ainsi la base de la collaboration intensive avec les cantons pour la phase de mise en œuvre.

Actuellement, de nombreux services sont offerts et utilisés via les canaux électroniques, ce qui augmente la présence de tous les acteurs dans l'Internet et leur dépendance à l'égard des infrastructures critiques[4]. L'économie est ainsi particulièrement vulnérable face aux cyberrisques, tels que les attaques à buts frauduleux, vénaux ou relevant de l'espionnage économique notamment. L'intégration de l'économie, en particulier des opérateurs d'infrastructures critiques, des fournisseurs de prestations TIC et des fournisseurs de systèmes, dans une stratégie de protection contre les cyberrisques est donc essentielle.

- Les cyberattaques contre des infrastructures critiques peuvent entraîner des conséquences particulièrement graves car elles menacent des fonctions vitales ou peuvent déclencher des réactions en chaîne. Les opérateurs (souvent privés) d'infrastructures critiques revêtent donc une signification toute particulière en tant que fournisseurs de services de très grande importance sur le plan de la sécurité.
- Les autorités et les administrations à tous les échelons (Confédération, cantons, communes) peuvent également être victimes de cyberattaques visant leurs fonctions législatives, exécutives ou judiciaires. Elles peuvent cependant aussi être la cible d'attaques dans leur rôle d'opérateurs et d'utilisateurs d'infrastructures critiques ou encore d'institutions de recherche.
- Les cyberrisques menacent également la population et tous les utilisateurs privés et professionnels de systèmes d'information et de communication ainsi que d'infrastructures critiques. Une stratégie efficace contre les cyberrisques doit donc prendre en compte le comportement individuel et les risques qui en découlent.

En premier lieu, ce sont les acteurs individuels qui sont responsables du maintien et de l'optimisation des mesures de protection visant à réduire les cyberrisques. Ces derniers sont en effet liés aux tâches, aux responsabilités et aux processus existants dans le cyberespace. Il est donc dans l'intérêt des utilisateurs d'élaborer et de mettre en œuvre des solutions adaptées à leurs besoins réels. Cette approche est aussi celle qui correspond le mieux à nos structures politiques et économiques décentralisées. L'Etat fournit des prestations subsidiaires de protection contre les cyberrisques, par exemple à travers l'échange d'informations et la contribution des services de renseignement. Dès que l'action individuelle ou sectorielle n'a pas d'effet, est inefficace ou impraticable, l'Etat est alors tenu de fournir

[4] Les infrastructures critiques sont des infrastructures dont la perturbation, l'interruption ou la destruction auraient des conséquences dramatiques sur la société, l'économie ou l'Etat. Les installations de contrôle et de commutation de la distribution d'énergie électrique et des télécommunications font, par exemple, partie des infrastructures critiques. Un inventaire des infrastructures critiques sera entrepris dans le cadre de la stratégie nationale pour la protection des infrastructures critiques.

des prestations subsidiaires supplémentaires de protection contre les cyberrisques afin d'appuyer les autres acteurs. La présente stratégie doit montrer où se trouvent les faiblesses du dispositif actuel pour contrer les cyberrisques ; elle décrit les prestations que l'Etat et les autres acteurs doivent assurer afin d'élever le niveau de protection de la Suisse.

Il s'agit cependant de réaliser que les efforts de protection peuvent entrer en conflit avec d'autres intérêts légitimes. Une base informative la plus complète possible, reposant sur des résultats technico-opérationnels et stratégico-politiques, doit être créée pour que des décisions motivées puissent être prises : il est possible qu'un conflit d'intérêts survienne dès lors que la création de redondances et de surcapacités, pour souhaitable qu'elle soit en termes de *protection* de certaines infrastructures, peut aller à l'encontre des *considérations économiques*. Par ailleurs, il convient de considérer les effets de la libéralisation qui a conduit, à cet égard, à une situation où un nombre croissant d'opérateurs d'infrastructures critiques (p. ex. énergie, télécommunications) sont désormais partiellement ou entièrement en mains privées et donc soumises prioritairement à une logique économique. Un second domaine où se manifeste un conflit d'intérêts est celui des *droits de la personnalité* : en effet, le renforcement des mécanismes de protection dans le cyberespace (p. ex. un contrôle ou une surveillance renforcés) doit être mis en balance avec la protection de la sphère privée. La présente stratégie a donc aussi pour but de prendre en compte ces intérêts divergents et de montrer quelles mesures peuvent être prises en agissant avec circonspection.

En cas de crise qui se manifeste par une attaque réussie ou une perturbation durable aux conséquences graves, une gestion de crise spécifique est nécessaire. En pareille situation, il s'agit prioritairement de faire interagir des actions au sein des structures existantes, actions qui doivent se dérouler en tenant compte de mesures politiques menées au niveau national et des lois applicables dans le cadre de la poursuite pénale. Dans un tel cas, la recherche des origines de la crise et l'amélioration de la capacité de résistance des infrastructures concernées sont également comprises dans la maîtrise des événements. En outre, les exploitants des infrastructures critiques, ainsi que les fournisseurs concernés de prestations TIC et de systèmes, sont, sur la base de conventions, parties prenantes dans ce processus.

La stratégie de protection de la Suisse contre les cyberrisques présente des interfaces avec d'autres projets à l'échelon de la Confédération qui traitent aussi de questions de sécurité et dont les sujets sont analogues. Ces travaux doivent être étroitement coordonnés dans la phase de mise en œuvre. Les principaux projets à cet égard sont énumérés ci-après.

Stratégie du Conseil fédéral pour une société de l'information en Suisse

La stratégie du Conseil fédéral pour une société de l'information en Suisse a été approuvée par le Conseil fédéral le 9 mars 2012. La Confédération met l'accent sur les mots d'ordre « sécurité et confiance ». Les objectifs qu'elle poursuit ainsi sont le développement des compétences de sécurité, la protection contre la cybercriminalité et l'augmentation de la résilience des TIC et des infrastructures critiques. Le concept qui y est rattaché, et qui a été approuvé par le Conseil fédéral en 2010 déjà, prévoit des mesures de sensibilisation de la population et des petites et moyennes entreprises afin qu'elles utilisent les TIC en étant conscientes des problèmes de sécurité, tout en restant conformes aux dispositions juridiques applicables en la matière.

Stratégie nationale de protection des infrastructures critiques

Le Conseil fédéral a chargé l'Office de la protection de la population (OFPP) de coordonner les travaux dans le domaine de la protection des infrastructures critiques (PIC). Se fondant sur la stratégie de base du Conseil fédéral de juin 2009 en matière de PIC, l'OFPP établit notamment une liste des infrastructures critiques en Suisse (inventaire PIC), permettant

aussi d'identifier des infrastructures critiques TIC. Il élabore, en outre, un guide d'amélioration de la protection globale (intégrale) des infrastructures critiques. La stratégie de base PIC est actuellement complétée par une stratégie nationale PIC qui sera soumise au Conseil fédéral en même temps que la présente stratégie.

Législation sur la sûreté de l'information au sein de la Confédération

Par décision du 12 mai 2010, le Conseil fédéral a chargé le DDPS d'élaborer des bases légales formelles pour la protection et la sûreté de l'information afin d'assurer la confidentialité, la disponibilité, l'intégrité et l'authenticité des données et informations. Cette nouvelle législation doit fixer en premier lieu les principes de la sûreté de l'information pour toutes les autorités fédérales et régler les responsabilités de manière uniforme. Il en découlera des directives concernant le traitement des données et informations devant être protégées. La procédure de consultation est prévue pour la fin 2012.

Rapport du Conseil fédéral relatif au postulat Malama (« Sécurité intérieure. Clarification des compétences »)

Suite au postulat Malama, demande a été faite au Conseil fédéral d'établir un rapport clarifiant les compétences constitutionnelles et la répartition effective des tâches entre la Confédération et les cantons en matière de sûreté intérieure. Il s'agissait, en particulier, d'examiner si la distribution des compétences est appropriée et si elle satisfait aux exigences actuelles. Le Conseil fédéral a approuvé le rapport le 2 mars 2012.

2 CYBERRISQUES

Les cyberrisques sont bien réels et divers. Même si l'on manque de détails précis et que l'on est souvent réduit à de simples appréciations générales sur leur importance, sur la fréquence des cyberattaques et des perturbations techniques, ainsi que sur la nature et l'ampleur des dommages effectifs ou des dommages possibles, la tendance des dernières années est absolument claire : les incidents où des Etats, des entreprises et des particuliers sont agressés et subissent des dommages via le cyberespace augmentent en quantité et en qualité.

Cette situation est une conséquence de la mise en réseau croissante des infrastructures TIC, de notre dépendance toujours plus grande à leur égard et de l'opacité des processus d'appui. La complexité croissante des systèmes d'information les rend de plus en plus sensibles aux erreurs et défaillances augmentant ainsi les possibilités de les attaquer. Il faut donc s'attendre à ce que les cyberattaques deviennent toujours plus professionnelles et dangereuses et qu'à côté des cas connus, de nombreuses attaques ne seront pas annoncées, voire pas découvertes. En effet, nombre de cas resteront non divulgués afin de préserver la réputation des entreprises attaquées.

2.1 Méthodes

Les cyberattaques sont conduites contre des ordinateurs, des réseaux ou des données. Elles ont pour but de porter atteinte à l'intégrité des données, de perturber des infrastructures, de limiter leur disponibilité ou d'interrompre leur fonctionnement. Ces attaques tendent notamment à compromettre la confidentialité et l'authenticité des informations en y accédant illégalement, en les effaçant ou en les modifiant, en surchargeant les liaisons ou les serveurs, en espionnant les contenus qui y transitent, ou encore en manipulant de façon ciblée les systèmes de surveillance ou de traitement.

Les instruments pour conduire les cyberattaques sont multiples. Il peut s'agir de programmes malveillants déposés intentionnellement dans des ordinateurs à l'insu de leur propriétaire afin de porter atteinte à la confidentialité, à l'intégrité ou encore à l'authenticité des données qui s'y trouvent. Des fonctions défaillantes dans des systèmes d'exploitation ou des applications insuffisamment protégées et entretenues (p. ex. navigateur Internet ou applications spécialisées) aident l'attaquant à prendre le contrôle des ordinateurs touchés. Ces systèmes peuvent ensuite être contrôlés à distance via une liaison Internet ou en y installant d'autres logiciels malveillants qui, à leur tour, permettront d'atteindre des données qui se trouvent dans le système, de les transmettre à l'attaquant, de les modifier ou de les détruire. Certaines données que des utilisateurs ont saisies en tapant sur les touches de leurs claviers peuvent, par exemple, être enregistrées et transmises à l'attaquant ou provoquer des attaques involontaires contre des sites peu protégés. De cette manière, un attaquant peut notamment avoir accès à des numéros de cartes de crédit, des services informatiques bancaires et d'autres données confidentielles. Les attaquants peuvent aussi tirer avantage des faiblesses que peuvent présenter l'organisation de certains concepts de sécurité des entreprises afin de pénétrer dans des systèmes protégés. Via les processus de gestion des données et des systèmes à la sécurité défaillante (dès la conception) ou mal entretenus (p. ex. en laissant le mot de passe initial), les attaquants parviennent souvent à pirater la plupart des systèmes.

Des ordinateurs ainsi sous contrôle peuvent ensuite être utilisés par les attaquants pour lancer des actions coordonnées massives sur des serveurs et en compromettre la disponibilité. Il s'agit d'attaques par déni de service (distributed denial-of-service attack).

Dans de nombreux cas, on observe des méthodes d'espionnage classiques visant à compromettre la confidentialité de données (p. ex. ingénierie sociale, vol ou effraction). Des utilisateurs de systèmes se font dérober par l'astuce des renseignements sur les mesures de sécurité usitées, des supports de données sont volés, des infrastructures manipulées sur place et leur configuration modifiée. Des méthodes classiques de sabotage peuvent aussi être mises en œuvre afin d'attaquer spécifiquement des installations industrielles de télégestion[5] en développant et en engageant des logiciels malveillants particuliers.

Les attaquants peuvent, en outre, bénéficier de caractéristiques spécifiques au cyberespace leur permettant de se soustraire à une détection (précoce), voire à des poursuites pénales (abouties) grâce à l'anonymat, à la distance géographique, aux obstacles juridiques, à la dissimulation et à l'effacement de traces par la falsification de données et à la complexité croissante des méthodes d'attaque. Souvent, il est pour ainsi dire impossible, à partir des méthodes d'attaques constatées et des instruments identifiés, de remonter à l'auteur et à ses motivations. Tous les attaquants disposent des mêmes méthodes et instruments, mais ils sont mus par des motivations différentes et mandatés par des donneurs d'ordre distincts.

Les cyberattaques les plus fréquentes sont faciles à réaliser pour les attaquants car les moyens et compétences techniques requis peuvent souvent être obtenus sans difficulté et à moindre coût. La plus grande partie des attaques relève du vandalisme non coordonné, de l'espionnage et d'actes frauduleux sur Internet, causant des dommages généralement limités (p. ex. atteinte à la réputation) et relativement faciles à réparer. Bien que la protection contre ce genre d'actes soit importante, la présente stratégie traite avant tout d'agressions pouvant causer des dommages de grande ampleur qui limitent fortement, directement ou indirectement, la capacité d'agir de l'économie, de l'Etat et de la société.

Avec des attaques spécifiques, aux coûts évidemment plus élevés, il est aussi possible d'infliger des dommages significatifs, même à des infrastructures particulièrement bien protégées.

Il est irréaliste de penser que l'on pourra parvenir à une protection absolue contre les cyberattaques. C'est pourquoi il est primordial que les capacités de réaction soient en harmonie avec les capacités de prévention ; ces capacités sont orientées vers une approche réduisant les risques et visant la limitation des dommages et la restauration de la situation initiale.

2.2 Acteurs et motivations

Les acteurs sont des individus, des groupes ou des Etats. Ils se différencient principalement par leurs motivations, ainsi que par leurs moyens techniques et financiers.

Les *acteurs étatiques ou financés par des Etats* disposent, en règle générale, de ressources humaines et de moyens financiers et techniques supérieurement importants ; ils sont bien organisés et sont ainsi en mesure d'infliger des dégâts majeurs. Par leurs attaques, ils cherchent à espionner, faire chanter, compromettre d'autres Etats, des autorités spécifiques,

[5] Sur le plan international, on parle de systèmes SCADA (*Supervisory Control and Data Acquisition*), c'est-à-dire de système de télégestion servant à la surveillance et au pilotage de processus techniques.

l'armée, l'économie ou des instituts de recherche. Ils ont également à dessein de s'attaquer à d'autres intérêts nationaux pour mener leur politique hégémonique ou poursuivre des intérêts économiques. Les entreprises, institutions ou personnes d'origine étrangère établies en Suisse sont également menacées.

> *En octobre 2009, on découvrait, au Département fédéral des affaires étrangères, un logiciel malveillant effectuant des activités d'espionnage. Il est arrivé dans le réseau via un courriel et est resté longtemps sans être détecté. Quelques années auparavant, les entreprises d'armement RUAG et Mowag ont été attaquées de la même manière. En juin 2010, un logiciel malveillant (Stuxnet) a été découvert ; il avait été vraisemblablement développé afin d'endommager des installations d'enrichissement d'uranium de l'Iran en introduisant une erreur dans les systèmes SCADA. En raison de sa complexité, on suppose que seuls des acteurs étatiques ont pu en être les auteurs.*

Les *acteurs de la criminalité organisée* peuvent représenter un niveau similaire de menace, car ils disposent souvent d'organisations professionnelles, d'importants moyens financiers et de capacités spécifiques. Leurs intentions d'enrichissement et leurs cyberattaques massives et continues contre l'économie (p. ex. le système financier) et les individus peuvent avoir pour conséquence d'importants dommages économiques, à tel point que la crédibilité de l'Etat peut même être remise en question.

> *Depuis plusieurs années, on observe, entre autres, les effets du cheval de Troie ZeuS[6] contre les transactions bancaires en ligne. Ce logiciel malveillant s'introduit dans les infrastructures informatiques des particuliers par des pages Web falsifiées ou manipulées. Les attaquants peuvent ensuite pirater le service de télépaiement et ainsi retirer de l'argent des comptes.*

Plus récemment, ce sont les attaques contre des portails Web du secteur privé ou public par de nouveaux acteurs appelés « *hacktivistes* » qui ont pris de l'importance. Ces organisations non étatiques, individuelles, parfois peu organisées, mais capables de disposer, selon les circonstances, d'une grande quantité d'acteurs, disposent de bonnes capacités techniques. Le potentiel de dégâts engendrés par des attaques massives provenant de ces acteurs est évalué comme moyen, voire élevé. Ces « hacktivistes » ont pour but d'interrompre des transactions, de provoquer des dégâts financiers ou de ternir l'image d'une entreprise afin d'attirer l'attention publique sur leurs revendications.

> *En décembre 2010, un groupe de hackers appelé « Anonymous» s'est attaqué à PostFinance, interrompant ainsi les services Internet durant toute une journée. La cause de cette action avait été la fermeture du compte de chèque postal du fondateur de WikiLeaks, Julian Assange. En 2007, en raison du déplacement contesté d'un mémorial militaire de l'époque soviétique à Tallinn, des activistes russes ont attaqué massivement les infrastructures TIC estoniennes. Les services d'administration en ligne et les services Internet de nombreuses entreprises ont été interrompus durant plusieurs jours et de nombreux portails officiels et d'entreprises ont été falsifiés avec de la propagande pro-russe.*

Les *mouvements terroristes* utilisent le cyberespace non seulement pour diffuser leur propagande, recruter, radicaliser et instruire leurs membres, mais aussi pour acquérir des moyens financiers, planifier leurs actions et communiquer. Jusqu'ici, ils ont utilisé les infrastructures TIC, mais ne les ont pas attaquées et ont toujours préféré les méthodes conventionnelles avec des attaques concrètes contre la vie et l'intégrité physique ainsi que

[6] Logiciel malveillant (*malware ou malicious software*).

contre des infrastructures. Les cyberattaques terroristes entraînant des dommages matériels importants restent, pour l'instant, encore peu probables. Il ne peut toutefois pas être exclu qu'à l'avenir des terroristes essaient de lancer des cyberattaques contre des infrastructures critiques d'un pays. Même si la Suisse n'est pas prise pour cible directe, elle pourrait ainsi être également touchée par les conséquences transfrontalières d'une telle attaque (p. ex. panne d'approvisionnement en électricité ou perturbation du marché financier).

> *Jusqu'ici, il n'existe pas d'exemple concret de cyberattentats terroristes. Toutefois, les sites Internet d'organisations terroristes ou de groupuscules de sympathisants sont constamment surveillés dans le but d'y repérer des appels à la violence ou des indications sur des attentats imminents (p. ex. les sites djihadistes).*

Du reste, des événements imprévisibles ou des accidents (p. ex. des pannes de systèmes) causés par une usure prématurée, une surcharge, un défaut de conception, un entretien insuffisant, ou les conséquences d'une catastrophe naturelle peuvent également conduire à des pannes ou perturbations d'infrastructures aux conséquences graves, similaires aux effets de cyberattaques.

3 STRUCTURES EXISTANTES

Les structures dont dispose la Suisse pour réduire les cyberrisques sont exposées ci-après et les rôles attribués aux différents acteurs sont passés en revue.

3.1 Economie et opérateurs d'infrastructures critiques

Acteurs concernés[7]

La place économique suisse se caractérise par un important secteur des services. Les relations et activités commerciales sont fondées, de par la chaîne de valeurs dans son ensemble, sur les infrastructures TIC. Les données sont stockées et exploitées sur des systèmes informatiques internes et externes aux entreprises. La communication et le trafic des paiements se fondent sur des prestations liées à l'Internet (p. ex. courriel, téléphonie via Internet, services d'e-banking et bourse). De plus en plus, les contrats sont aussi conclus par voie électronique (commerce sur Internet, procédures d'offres, etc.). Cela illustre bien à quel point notre économie dépend du bon fonctionnement des TIC et des autres infrastructures critiques, comme l'alimentation en courant électrique. C'est pourquoi la protection face aux cyberrisques revêt une importance nationale pour notre place économique.

Les infrastructures critiques garantissent la disponibilité de biens et de prestations essentielles. De graves perturbations, voire l'arrêt, de telles infrastructures auraient des conséquences graves sur le fonctionnement de l'Etat, de l'économie et de la société. Protéger les infrastructures critiques – notamment contre les cyberrisques – est donc essentiel. Les opérateurs d'infrastructures critiques ne peuvent dès lors pas uniquement considérer les risques sous un angle économique ; ils doivent également entreprendre des efforts pour réduire leur exposition à ceux-ci et sont déjà soumis à des règles particulières dans ce sens. Toutefois, les directives concrètes et contraignantes en matière de standards de protection des TIC utilisées font généralement défaut. En fonction de la criticité et de la vulnérabilité d'une infrastructure et de la menace, des normes de sécurité et des mesures de réduction des risques plus précises et exhaustives devraient être fixées en association avec les organes compétents.

Les producteurs et fournisseurs de produits et de prestations TIC portent une grosse responsabilité en ce qui concerne la sécurité de leurs produits et, par extension, la cybersécurité de leurs clients.

Les acteurs économiques agissent, pour la plupart, en fonction de leur responsabilité et de leur jugement individuels. Afin de se faire une idée globale de la situation, des entreprises choisies pour l'élaboration de la stratégie ont été interrogées sur leur appréciation de la situation, sur les mesures prises, sur les difficultés rencontrées, ainsi que sur les développements des normes de sécurité prévues dans le domaine de la cybersécurité.

Perception du problème

[7] Le DDPS a conduit une enquête auprès de représentants de l'économie et d'opérateurs d'infrastructures critiques (y. c. des organisations faîtières et professionnelles) concernant les mesures adoptées en matière de cybersécurité, les lacunes et difficultés constatées et les facteurs influençant la mise en place de leurs mesures de précaution (p. ex. en termes financiers). Dans l'ensemble, cette enquête a fourni une image unitaire.

Les cyberrisques sont incontestablement un thème majeur pour les entreprises. Cependant, l'appréciation des risques et les mesures prises varient fortement d'un secteur de l'économie à l'autre, mais aussi au sein des diverses branches et entreprises. Une classification sectorielle de la perception du problème n'est donc pas possible.

Certaines entreprises ont une perception très vive du problème. Dans cette catégorie, on compte surtout de grandes entreprises disposant de moyens importants en termes de capital, de personnel, d'infrastructures et de savoir-faire (p. ex. en matière de forensique, de gestion des risques et gestion de crise, de CERT [Computer Emergency Response Teams]). Ces entreprises sont souvent actives sur le plan international et disposent d'un grand réseau relationnel. Les entreprises actives dans la sécurité (p. ex. l'industrie de l'armement), et dont les besoins en termes de sécurité sont accrus, sont, en règle générale, en mesure de faire face seules aux menaces qui frappent quotidiennement la Suisse.

Les opérateurs d'infrastructures critiques font également partie des acteurs qui accordent une grande attention aux cyberrisques. Ils attendent cependant des autorités de régulation qu'elles émettent, en collaboration avec eux et en fonction de leur criticité et de leur vulnérabilité, des exigences complètes et précises en matière de sécurité.

Le plus grand groupe comprend des petites et des moyennes entreprises (PME) disposant d'une perception moyenne du problème et qui utilisent, la plupart du temps, simplement les solutions commerciales disponibles (p. ex. pare-feu et programmes antivirus). Leur capacité à améliorer leurs mesures de protection dans le cyberespace est principalement fonction de leurs moyens financiers.

Enfin, on observe un troisième groupe : celui des entreprises n'ayant qu'une faible perception du problème. Elles n'accordent que peu ou pas de ressources pour les mesures de protection, n'en voyant pas ou n'en comprenant pas la nécessité.

Mesures

Seule une minorité d'acteurs économiques peut faire face à des cyberattaques de haute intensité (en termes de simultanéité, complexité, potentiel de dégâts ou durée).

De nombreuses entreprises connaissent et appliquent les normes de sécurité (p. ex. ISO 2700x, NERC). Elles prennent aussi des précautions techniques ou organisationnelles (p. ex. exploitation de systèmes autonomes, engagement de responsables de la sécurité), ainsi que des mesures pour améliorer la perception du besoin de sécurité de leurs collaborateurs, mais négligent souvent celle des décideurs. Ces mesures contribuent à l'identification des faiblesses internes, à l'exploitation et à l'amélioration continue sur le long terme des mesures de sécurité. La plupart des PME font cependant peu dans ce domaine. La qualité de la prise en compte des risques est souvent déterminée par des considérations économiques. Les cyberrisques font partie intégrante de processus d'entreprises globaux et ne peuvent donc pas être combattus isolément ou uniquement sur le plan technique. A cela s'ajoute le fait que les bases informatives pour la prise de décision présentent fréquemment des lacunes et que les informations spécifiques au cyberespace apparaissent marginalement. Pour parvenir à un niveau de protection avec le moins de failles possible et ne faussant pas les conditions de concurrence, les entreprises et les opérateurs d'infrastructures critiques exigent que des normes et directives unitaires soient développées et mises en œuvre en collaboration avec tous les milieux concernés et leurs responsables.

L'optimisation de l'échange d'informations entre les acteurs de l'économie, en particulier les opérateurs d'infrastructures critiques, les fournisseurs de prestations TIC, les fournisseurs de systèmes et les autorités, est déterminante pour résoudre les problèmes et limiter les

dommages. On constate cependant que la collaboration avec l'extérieur est réduite (y. c. avec les autorités). Les grandes associations économiques ne se sont jusqu'ici que peu penchées sur le thème de la cybersécurité et sur le rôle qu'elles ont à jouer dans ce domaine. L'enquête montre qu'il existe un besoin de développer et de consolider des formes de collaboration entre l'économie et les autorités pour procéder à des échanges de données sur la situation et prendre des mesures dans le cadre de la gestion des crises[8]. Malheureusement, les cyberattaques constatées sont souvent tues, ce qui prive les autres victimes potentielles de recevoir à temps des mises en garde. Les entreprises et les opérateurs d'infrastructures critiques interrogés réclament une collaboration fondée sur une participation facultative. Si la responsabilité individuelle reste fondamentale, la collaboration, elle, doit permettre de pallier ensemble les failles éventuelles et d'obtenir des informations en rapport avec la situation afin de permettre à chacun d'appuyer sa propre gestion des risques.

Des progrès significatifs ont été réalisés, ces dernières années, en matière de collaboration entre la Confédération, les opérateurs d'infrastructures critiques, les fournisseurs de prestations TIC et les fournisseurs de systèmes pour réduire les cyberrisques. Une collaboration est en place pour la planification stratégique à long terme, l'analyse des risques et la gestion de la continuité, en premier lieu entre l'Office fédéral de l'approvisionnement économique, les cantons, une partie des infrastructures critiques, les fournisseurs de prestations TIC et les fournisseurs de systèmes. Un partenariat entre secteur public et secteur privé (Public Private Partnership) a été établi avec la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) de la Confédération, les cantons et l'économie privée. MELANI appuie les opérateurs d'infrastructures critiques dans leur processus de sûreté de l'information et favorise l'échange d'informations en matière de cyberattaques ; ses ressources ne lui permettent toutefois qu'imparfaitement de remplir ses missions. Il est donc nécessaire de traiter prioritairement la question de savoir dans quelle mesure cette institution devra assurer, à l'avenir, la demande d'appui sans cesse croissante des opérateurs d'infrastructures et quel impact cela aura sur ses ressources.

Les faibles marges bénéficiaires et la forte concurrence internationale ne permettent pas d'imposer des exigences plus poussées en termes de sécurité qui soient applicables à la Suisse uniquement. Les surcoûts générés pénaliseraient trop la compétitivité de l'économie suisse. Les directives en matière de protection dans ce domaine et les solutions de mise en œuvre doivent donc être développées en considérant le contexte international. La collaboration à ce niveau ne doit toutefois pas être intensifiée uniquement en termes de normes et de prescriptions. Elle doit l'être également en matière d'identification des risques et de gestion commune des crises, non seulement entre Etats, mais aussi en intégrant les représentants de l'économie (tout particulièrement les opérateurs d'infrastructures critiques, les fournisseurs de prestations TIC et les fournisseurs de systèmes) et de la société civile.

Le manque de spécialistes en cybersécurité ainsi que l'acquisition et le maintien du savoir spécifique requis représentent également des défis importants. Les entreprises et opérateurs d'infrastructures critiques interrogés souhaitent instamment l'encouragement de la recherche et du développement en la matière, ainsi que le recrutement et la formation de spécialistes.

---

[8] Voir à ce propos l'étude « Evaluation et développement de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) » publiée en 2012 par l'EPF de Zurich. Elle vérifie l'efficacité de MELANI, compare la centrale à des modèles internationaux de sûreté de l'information et en tire des possibilités de développement et des recommandations.

3.2 Confédération

Ces dernières années, la Confédération a pris diverses mesures pour renforcer les moyens et le dispositif de sécurité de l'administration fédérale contre les cyberattaques, et diverses organisations (voir ci-après) sont en charge de tâches préventives et réactives dans le domaine de la cybersécurité au niveau de la Confédération.

Ministère public de la Confédération (MPC)

Le MPC est l'organe d'enquête et de poursuite pénale de la Confédération. Il est responsable de la poursuite des actes illicites soumis à la juridiction fédérale (la plupart des actes délictueux relèvent de la compétence des cantons) et de la coopération avec l'étranger.

Préposé fédéral à la protection des données et à la transparence (PFPDT)

Le PFPDT est un service de surveillance, d'information et de conseil pour les organes de la Confédération et les particuliers. Son rôle consiste essentiellement à expliquer la loi sur la protection des données et les ordonnances d'exécution. Il prodigue des conseils relatifs aux questions d'ordre juridique ainsi qu'à des aspects techniques de la sécurité des données.

Etat-major pour la sûreté de l'information (SONIA)

L'Etat-major spécial pour la sûreté de l'information rassemble des décideurs de l'administration et de l'économie (opérateurs d'infrastructures critiques). Il est dirigé par le délégué de l'UPIC et entre en action sur demande de MELANI en cas de crise nationale en relation avec la protection de l'information. Actuellement, SONIA n'est que partiellement opérationnel, notamment depuis le dernier exercice réalisé en 2005 qui a démontré que sa structure et ses processus ne sont pas fonctionnels dans la pratique. En cas de crise, les membres prévus pour cet état-major seraient, en effet, déjà impliqués dans d'autres processus, de gestion de crises notamment.

Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI)

MELANI est un organe conjoint de l'UPIC, l'Unité de pilotage informatique de la Confédération (pilotage de MELANI et du Government Computer Emergency Response Team, GovCERT[9]) et du SRC (*Operations and Information Center*). MELANI appuie subsidiairement le processus de sécurisation de l'information des infrastructures critiques en informant leurs opérateurs des incidents survenus et des menaces. Elle récolte des informations, techniques et non techniques, les analyse et diffuse les données pertinentes aux opérateurs d'infrastructures critiques. En rendant, par exemple, ses appréciations de la situation et ses analyses prévisionnelles d'attaques et d'incidents disponibles, en évaluant leurs répercussions et en analysant au besoin des logiciels malveillants, MELANI appuie le processus de gestion des risques des infrastructures critiques.

Pour l'heure, MELANI seconde uniquement un groupe restreint d'entreprises sélectionnées exploitant des infrastructures critiques en Suisse (100 participants env., tels que banques, entreprises de télécommunication et d'approvisionnement en énergie). MELANI apporte son

[9] Les CERT sont des organisations responsables de l'analyse technique d'incidents. Ils récoltent et analysent les informations techniques dans le contexte général d'un événement et assurent un rôle de coordination. Une telle organisation existe au niveau de la Confédération. Il s'agit du GovCERT qui assure en plus une fonction de coordination sur le plan international.

aide aux autres acteurs de l'économie et à l'ensemble de la population en leur proposant des listes de contrôle, des instructions et des programmes d'apprentissage. En cas de crise, MELANI est responsable de l'alarme et de l'aide au commandement de l'Etat-major spécial pour la sûreté de l'information (SONIA). En raison de ses ressources humaines limitées, MELANI ne parvient toutefois que partiellement à assurer sa mission de base.

Département fédéral de justice et police (DFJP)

Office fédéral de la police (fedpol)

Police judiciaire fédérale (PJF)

La PJF est un organe d'enquête de la Confédération. Dans son domaine de compétences, elle assume des tâches de police criminelle et de police judiciaire qui servent à l'identification, à la lutte et à la poursuite d'infractions qui ont été commises. Elle assure la collaboration entre les partenaires nationaux et internationaux et suit notamment le développement technique de la cybercriminalité. Elle garantit également le maintien et le développement des compétences forensiques dans ce domaine. La PJF n'est responsable, en tant que police judiciaire, que des événements qui relèvent de la compétence fédérale. Si la compétence fédérale ou cantonale n'est pas clairement établie, elle est habilitée à conduire des enquêtes préliminaires et assure la coordination pour les cas concernant plusieurs cantons.

Service de coordination de la lutte contre la criminalité sur Internet (SCOCI)

Le SCOCI est une organisation conjointe de la Confédération et des cantons, responsable d'identifier à temps les infractions commises sur Internet, d'éviter les doublons en matière de poursuite pénale et d'analyser la criminalité sur Internet[10]. Le SCOCI est rattaché à fedpol. Il est le point de contact pour les personnes qui souhaitent annoncer des contenus suspects sur Internet. Après un premier examen et une sauvegarde des données, ces annonces sont ensuite transmises aux autorités pénales compétentes en Suisse et à l'étranger. Le SCOCI est au service du public, des autorités et des fournisseurs d'accès Internet pour répondre à toute question juridique, technique et criminelle relative à la criminalité sur Internet. Il recherche également activement des contenus illicites sur Internet, notamment dans les domaines de la pédophilie et de la criminalité économique (fraudes à la carte de crédit, appâtage par courriel, etc.) Le SCOCI est responsable du développement des techniques d'enquête et, avec le soutien des cantons et des autorités fédérales actives dans ce domaine, de l'établissement de la vue d'ensemble des processus et de l'évolution du droit en matière de criminalité sur Internet. Il est aussi l'interlocuteur privilégié des services étrangers exerçant la même fonction. Avec MELANI, le SCOCI assure l'échange des informations pertinentes du cyberespace entre les autorités pénales et le service de renseignement.

Coopération policière internationale (CPI)

La CPI est notamment responsable, via la centrale d'engagement de fedpol, des contacts avec les partenaires nationaux et internationaux. La collaboration stratégique et opérationnelle avec des unités et organisations policières

[10] Voir à ce propos la convention administrative du 19 décembre 2001 sur la coordination de la lutte contre la criminalité sur Internet et le règlement de gestion du 30 mars 2011 du service de coordination de la lutte contre la criminalité sur Internet.

internationales (EUROPOL, INTERPOL, ONU, OSCE, Conseil de l'Europe) lui incombe également.

Centrale d'engagement de l'Office fédéral de la police

La Centrale d'engagement de l'Office fédéral de la police est l'organe de contact permanent pour les instances compétentes étrangères. Elle appuie notamment les enquêtes pénales en Suisse et à l'étranger en matière de criminalité informatique. La centrale d'engagement ne peut pas, à elle seule, prendre de mesures en matière de conseil et d'assistance juridique, de relevé de preuves, de sauvegarde de données ou de procédure pénale. En tant qu'organe de contact, elle a toutefois pour mission de faciliter les relations entre les autorités nationales et internationales compétentes (en particulier le SCOCI).

Collaboration stratégique

La division de collaboration stratégique a pour tâche principale de développer la collaboration internationale avec des partenaires de la police. En accord et en coordination avec les services spécialisés de fedpol, elle représente l'Office fédéral de la police lors de conférences et de commissions bilatérales et multilatérales, ce qui lui permet notamment de suivre les derniers développements de la lutte contre la cybercriminalité.

Département fédéral de la défense, de la protection de la population et des sports (DDPS)

Service de renseignement de la Confédération (SRC)

Le SRC cherche et collecte des informations avec les moyens du renseignement, les analyse et les diffuse. En Suisse, le SRC se concentre sur les thèmes du terrorisme, de l'extrémisme violent, de la prolifération, des attaques contre les infrastructures critiques et le renseignement prohibé ; à l'étranger, il s'intéresse aux questions de politique de sécurité, entre autres à la prolifération, au terrorisme, au développement des forces armées, aux technologies de l'armement et au commerce des armes, ainsi qu'aux analyses stratégiques. Ces thèmes étant de plus en plus présents dans le cyberespace, le SRC y suit donc également le développement de la situation en matière de risques. Le SRC dirige, en collaboration avec l'UPIC, les organes de MELANI consacrés au renseignement.

Office fédéral de la protection de la population (OFPP)

L'objectif de la protection de la population est de protéger la population, de préserver les bases nécessaires à son existence en cas de catastrophe, de situation d'urgence ou de conflit armé, ainsi que de contribuer dans une large mesure à limiter et maîtriser les effets d'événements dommageables. Des catastrophes et des situations d'urgence peuvent aussi résulter de cyberattaques graves ou d'autres perturbations des TIC. En conséquence, les travaux menés dans le cadre de l'analyse nationale des dangers « Risques Suisse » qui servent de base de planification pour la protection de la population rendent aussi compte des menaces liées au cyberespace. Dans le cadre du programme de protection des infrastructures critiques, l'OFPP coordonne, sur mandat du Conseil fédéral, les travaux d'établissement de l'inventaire PIC consistant à répertorier d'une part les infrastructures TIC critiques, et d'autre part les applications TIC sensibles au niveau de la sécurité dans les autres secteurs d'infrastructures critiques. La Centrale nationale d'alarme (CENAL), rattachée à l'OFPP, doit, en tant que centre fédéral d'annonce et de suivi de la situation en cas d'événement extraordinaire, pouvoir impérativement compter, en situation de crise, sur

des systèmes informatiques, des réseaux de communication et une alimentation électrique sans coupure. A l'avenir, la communication en matière de conduite entre les organes fédéraux et cantonaux (POLYCONNECT/POLYDATA) devrait se faire via des réseaux fiables en cas de crise et exempts de coupures en alimentation électrique. L'alerte et l'alarme (POLYALERT) commutent actuellement aussi vers une technologie fiable en cas de crise qui se fonde sur le réseau radio national de sécurité (POLYCOM).

Domaine Défense

Le domaine Défense du DDPS est responsable de la défense, du soutien aux autorités civiles et de la promotion de la paix.

Les organisations ci-après sont tout particulièrement responsables des tâches de protection liées à la défense.

Protection des informations et des objets (PIO)

La PIO, rattachée à l'Etat-major de l'armée, s'occupe de la sécurité intégrale du DDPS. Elle est notamment chargée des directives en matière de sécurité des personnes, des informations, de l'informatique, ainsi que des biens matériels et immobiliers.

A ce titre, elle élabore des directives en matière de sécurité pour assurer la confidentialité, la disponibilité, l'intégrité et la traçabilité d'informations et de données, ainsi que la disponibilité et l'intégrité de moyens TIC.

Elle exploite l'organe de coordination pour la protection des informations au sein de la Confédération et elle est l'interlocutrice principale pour toute question nationale ou internationale à propos de la protection des informations classifiées. Sur la base de quelques accords internationaux (notamment avec l'UE), la PIO est reconnue comme l'autorité nationale de sûreté pour tout ce qui concerne la sûreté de l'information.

Elle prend actuellement une part prépondérante dans l'élaboration d'une loi sur la sûreté de l'information au sein de la Confédération.

Base d'aide au commandement de l'armée (BAC)

La BAC est le fournisseur de prestations TIC de l'armée dans toutes les situations, ce qui nécessite en permanence une sécurité et une disponibilité élevées. Elle exploite le centre des opérations électroniques (COE) qui fournit des prestations au profit des services de renseignement. Le COE emploie des cryptologues et il est responsable du domaine des opérations dans les réseaux informatiques (CNO) qui dispose ainsi de capacités techniques d'analyse de la menace et des incidents et de capacités en matière de conduite des opérations. La BAC exploite, en outre, le Computer Emergency Response Team militaire (milCERT), lequel est responsable de la surveillance des infrastructures TIC de l'armée. La BAC soutient prioritairement l'armée, mais aussi la conduite politique et tient à leur disposition les moyens appropriés.

Renseignement militaire (RM)

Au sein de l'armée et du domaine Défense, le RM est compétent en matière d'acquisition d'informations destinées aux utilisateurs militaires. Le RM se charge de tout ce qui a trait au renseignement lors des engagements. Il bénéficie, pour ce faire, de l'aide du renseignement intégré et travaille en étroite collaboration avec l'Etat-major de conduite et les formations impliquées.

Le RM entretient des contacts internationaux avec des services de renseignement militaire et des agences (p. ex. OTAN). Il est ainsi rapporteur d'informations pour le SRC et l'appuie en lui fournissant des résultats concernant les cyberrisques et l'impact de la cybernétique dans l'environnement militaire. Dans le cadre d'engagements de contingents à l'étranger, le RM est, en outre, responsable du contre-espionnage et de sa présence dans le cyberespace.

Département fédéral des finances (DFF)

Unité de pilotage informatique de la Confédération (UPIC)

L'UPIC édicte des directives concernant les TIC et assure la gestion centralisée des prestations informatiques employées dans l'administration fédérale (p. ex. télécommunications). L'UPIC dirige aussi le GovCERT et la partie stratégique de MELANI. En cas de crise, elle chapeaute également l'Etat-major pour la sûreté de l'information (SONIA). En cas d'attaque contre les infrastructures TIC de l'administration fédérale, l'UPIC peut ordonner des mesures de sécurité supplémentaires.

Office fédéral de l'informatique et de la télécommunication (OFIT)

L'OFIT est un fournisseur de prestations en matière d'information et de télécommunication au sein de l'administration fédérale. Il dispose de son propre Computer Security Incident Response Team (CSIRT) qui collabore étroitement avec MELANI et d'autres organes de l'administration fédérale. Le CSIRT de l'OFIT surveille en permanence les ressources TIC de l'administration fédérale pour y détecter des attaques éventuelles et dispose d'une vaste expérience du traitement d'attaques de grande ampleur contre les infrastructures de la Confédération. Si la situation se détériore en termes de nombre d'incidents, d'intensité des attaques ou d'ampleur des dommages, l'OFIT ne dispose pas des ressources humaines nécessaires pour y faire face.

Gestion des risques de la Confédération

La gestion des risques a été introduite à la Confédération en 2005. Les buts et principes de la gestion des risques de la Confédération et ses différentes fonctions sont fixés dans les directives du 24 septembre 2010 sur la politique de gestion des risques menée par la Confédération[11]. Afin d'assurer une application homogène de la gestion des risques au sein de l'administration fédérale, le Département fédéral des finances (DFF) a fixé uniformément les détails y afférents qui ont force obligatoire dans des directives en date du 21 novembre 2011. Par « risque », on entend les incidents et développements dont le degré de probabilité de survenance est relativement élevé et dont les effets financiers et non financiers principaux se répercutent négativement sur les possibilités d'atteindre les objectifs et d'accomplir les tâches d'administration fédérale. La détection précoce de ces risques revient aux organes spécialisés des unités administratives et des départements. Les risques identifiés sont alors analysés, puis évalués. Les mesures nécessaires sont prises en fonction des résultats de l'exposition aux risques ; elles doivent permettre, si possible, d'éviter les risques ou du moins de les réduire. L'application du principe de la gestion des risques de la Confédération, orientée vers la spécificité des tâches, se déroule essentiellement de façon décentralisée au sein des unités administratives et des départements où les organes spécialisés sont chargés

[11] FF 2010 5965

de la détection précoce et de la défense contre les cyberattaques dirigées contre l'administration fédérale. Comme tous les départements et unités administratives de la Confédération sont concernés, le risque « cyberattaques contre les systèmes TIC de la Confédération » est géré au niveau fédéral comme un risque transversal.

Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC)

Office fédéral de la communication (OFCOM)

L'OFCOM s'occupe notamment de questions en lien avec les télécommunications. Dans ce domaine, l'OFCOM assure toutes les tâches régulatrices relevant de la souveraineté de l'Etat. Il assume en particulier la surveillance générale des télécommunications, y compris celle des fournisseurs d'accès à Internet (ISP). Il est également responsable des ressources d'adressage dans le domaine des télécommunications, ressources qui comprennent le contrat de droit administratif avec Switch, le service d'enregistrement des noms de domaines terminant par .ch, la surveillance s'y rapportant et les documents de référence pour la signature électronique. L'OFCOM est aussi très actif sur le plan international, tout particulièrement dans le domaine de la gouvernance d'Internet et des directives internationales. En outre, l'OFCOM coordonne, au niveau national et international, les activités conduites dans le cadre de la stratégie du Conseil fédéral pour une société de l'information en Suisse.

Office fédéral de l'énergie (OFEN)

L'OFEN est le centre de compétences pour toute question liée à l'approvisionnement en énergie et à la consommation d'énergie. Il crée les conditions nécessaires à un approvisionnement en énergie suffisant, fiable en cas de crise, très diversifié, économique et durable, et veille au respect des normes de sécurité élevées dans le cadre de la production, du transport et de l'utilisation d'énergie.

L'utilisation croissante de TIC dans les installations de production d'énergie et dans l'Internet entraîne une augmentation de l'exposition aux cyberrisques dans ces domaines.

Office fédéral de l'aviation civile (OFAC)

L'OFAC est compétent en matière de législation et de surveillance portant, entre autres, sur les aéroports, les compagnies aériennes et la sécurité aérienne en Suisse. Les conséquences possibles d'une cyberattaque sur l'aviation font de plus en plus l'objet d'une attention toute particulière, si bien que des dispositions de réduction des cyberrisques sont prises dans diverses réglementations. A cet égard, l'OFAC est responsable de l'intégration de ces dispositions dans le programme national de sécurité de l'aviation et les applique d'entente avec l'industrie.

Département fédéral de l'économie (DFE)

Approvisionnement économique du pays (AEP)

L'approvisionnement économique du pays est une organisation de milice disposant d'une organisation d'état-major et d'un secrétariat permanent (Office fédéral pour l'approvisionnement économique du pays, OFAE). L'AEP est composée de cadres provenant de l'économie. Le domaine des infrastructures TIC (ICT-I) de l'AEP est chargé d'assurer l'approvisionnement du pays en matière d'infrastructures d'information (production, transmission, sécurité et disponibilité de données) et de télécommunications, en particulier avec l'étranger. Il définit quelles infrastructures d'approvisionnement sont significatives pour la Suisse et établit à leur intention un processus de gestion de la continuité et des crises. Le domaine ICT-I observe et analyse en permanence les risques globaux de la transmission, de la sécurité et de la disponibilité des données. En situation d'urgence, il prend des mesures pour assurer les télécommunications avec les partenaires mobiles à l'étranger qui sont importants pour l'approvisionnement du pays. Il prend également des dispositions pour garantir le fonctionnement des infrastructures TIC vitales et assure la disponibilité requise pour l'approvisionnement de base. Il représente aussi les intérêts sectoriels de l'AEP au sein d'organisations internationales.

Département fédéral des affaires étrangères (DFAE)

Le Département fédéral des affaires étrangères (DFAE) structure et coordonne, sur mandat du Conseil fédéral, la politique étrangère de la Suisse.

La Direction politique du département suit l'évolution de la politique de sécurité à l'étranger dans le domaine des nouvelles formes de menaces et entretient des relations avec des organisations internationales – comme l'ONU, l'OSCE, l'UE, le Conseil de partenariat euro-atlantique (CPEA) et l'OTAN – qui, dans le cadre de leur politique de sécurité, sont de plus en plus confrontées aux menaces dans le cyberespace. Elle noue également des contacts avec ces organisations, thématise bilatéralement la cybermenace avec d'autres Etats et crée ainsi, au niveau politique, une base permettant à la Suisse de coopérer à la maîtrise de ce type de menace.

La Direction du droit international public traite les répercussions sur le droit international public des menaces survenant dans le cyberespace.

Conclusions intermédiaires

Au niveau de la Confédération, les structures pour la maîtrise des cyberrisques ont, jusqu'à présent, été organisées de manière décentralisée. Les moyens déployés sont modestes et les ressources ne suffisent souvent pas pour assumer des tâches supplémentaires. Les tâches dans ce domaine sont le plus souvent attribuées aux unités organisationnelles dont les missions attestent d'une forte présence dans le cyberespace. Cette organisation a un avantage essentiel : l'implication d'organes spécifiques nécessaires pour surmonter un incident se fait au cas par cas. Comme chaque attaque dirigée contre des infrastructures TIC se déroule différemment, la souplesse de l'organisation pour les cas d'urgence revêt une importance capitale et correspond à l'hypothèse selon laquelle la problématique de la cybernétique ne constitue pas un phénomène bien limité, mais doit être abordée dans le cadre de processus existants. En outre, cette organisation favorise les synergies et évite la

mise en place de structures lourdes avant que l'on sache exactement en quoi consiste la situation d'urgence. Ce système fonctionne donc bien sur le plan réactif. Il a montré qu'il disposait de capacités d'anticipation et de prévention, mais on s'aperçoit qu'elles sont désormais insuffisantes (p. ex. ressources humaines et financières ; échanges d'informations émanant des services de renseignement et de la police, ainsi que d'informations techniques pour soutenir l'économie, les opérateurs d'infrastructures critiques, les fournisseurs de prestations TIC, les fournisseurs de systèmes et la recherche ; analyses des risques et définitions des exigences qui en découlent en matière de sécurité, capacité à tenir dans le temps). Il s'agit donc de renforcer les structures décentralisées existantes au niveau de la Confédération en toute connaissance de cause et de mieux utiliser de possibles synergies afin de pouvoir identifier la globalité des cyberrisques et d'être en mesure de répondre aux exigences imposées par les cyberattaques et les perturbations de grande ampleur.

3.3 Cantons

Les cantons, comme les divers secteurs de l'économie, se caractérisent par leur grande hétérogénéité. En termes de population, certains cantons sont à peine plus grands que des villes de moyenne importance. On constate également de grandes différences entre eux sur le plan économique et structurel. Les prestations qu'ils fournissent et les activités et structures qu'ils offrent (p. ex. dans les domaines de la santé, des transports et de l'énergie) divergent donc autant que leurs besoins respectifs face aux menaces et dangers. Il va donc sans dire que les cantons ne disposent pas tous, qualitativement et quantitativement parlant, des mêmes compétences pour contrer les risques, en particulier dans le cyberespace.

La souveraineté des cantons s'étend à la préservation de la sécurité et de l'ordre public. Or, seuls les cantons disposant d'un corps de police conséquent et collaborant étroitement avec l'économie et d'autres organisations impliquées dans le domaine de la sécurité (comme les douanes, les services de sécurité des pays voisins) sont capables d'anticiper les problèmes dus à la cybercriminalité, de collecter les informations nécessaires et de mener de vastes enquêtes. Aucun canton n'est cependant en mesure de le faire systématiquement. Raison pour laquelle ils ont tous besoin de l'appui subsidiaire de la Confédération – en particulier dans les affaires concernant les services de renseignement et celles nécessitant une bonne coordination.

Les mesures préventives prises par les cantons pour limiter les cyberrisques font partie intégrante d'un concept global dans lequel elles occupent une place essentielle puisque tous les cantons exploitent des infrastructures critiques. Ils disposent généralement de structures d'organisation et de contrôle, de préposés à la sécurité dans divers services, de spécialistes de police forensique informatique ou de cellules de commandement en cas de crise. Souvent, toutefois – comme au niveau de la Confédération – ces moyens ne sont pas suffisamment coordonnés et ne permettent pas d'affronter globalement les cyberrisques actuels. Le problème est plus aigu dans les petits cantons qui sont souvent contraints de déléguer certaines prestations spécifiques à des tiers.

Force est également de constater que les dispositions juridiques régissant les technologies de l'information ne sont souvent pas suffisantes ou ne sont pas assez connues. Les systèmes de classification (INTERNE, CONFIDENTIEL, SECRET) ne sont pratiquement pas appliqués et les données sensibles (données personnelles, policières ou judiciaires) sont gérées dans des systèmes insuffisamment protégés.

Certains cantons sensibilisent déjà leur population à la prévention des dangers sur Internet par des campagnes spécifiques, p. ex. dans les écoles. Dans le contexte intercantonal, la Prévention suisse de la criminalité agit de même. De nombreux cantons restent cependant

inactifs ou comptent, dans ce domaine, sur les initiatives individuelles – et non coordonnées – du personnel enseignant ou des institutions de formation. Par ailleurs, les offres de programmes de la branche des TIC sont peu sollicitées, leur existence n'étant pas toujours connue.

Les cantons disposent d'organisations de conduite en cas de crise. Ces états-majors s'exercent régulièrement avec des partenaires (p. ex. avec les commandements militaires des régions territoriales) et sont en mesure de maîtriser les effets de crises de tout ordre. Ils ne traitent toutefois pas spécifiquement des cyberrisques et ne pourraient souvent pas apporter un soutien compétent aux milieux économiques et à la population en cas de cyberattaque.

Pour mettre en œuvre la stratégie nationale de protection contre les cyberrisques, les cantons et la Confédération disposent de plusieurs instruments pouvant fournir une contribution importante dans ce domaine. Ces instruments sont les suivants :

- la Maison des cantons, qui réunit sous un même toit plusieurs conférences intercantonales, gouvernementales et directoriales, notamment dans les domaines de la justice, de la police, de la protection de la population, de l'éducation, des finances et de la santé, ainsi que d'autres institutions comme la Prévention suisse de la criminalité ;
- le réseau national de sécurité, actuellement en cours de développement, qui coordonnera et rationalisera les activités des cantons et de la Confédération dans le domaine de la sécurité ;
- le programme d'harmonisation des moyens informatiques de la police, dont le but est de faire concorder les applications les unes avec les autres et de faciliter ainsi le travail de la police ;
- le Service de coordination de la lutte contre la criminalité sur Internet (SCOCI), financé et exploité conjointement par la Confédération et les cantons, qui surveille le cyberespace et livre des informations aux cantons pour le déclenchement des enquêtes de police ;
- en complément aux organes et groupes étatiques, il existe l'association Swiss Police ICT qui met en réseau directement et de manière spécifique différents corps de police et représentants du secteur des TIC. Son congrès, le Congrès informatique de la police suisse (SPIK), fournit en tant que plateforme une contribution importante dans le cadre des échanges d'informations concernant l'informatique de la police et la maîtrise des cyberrisques.

3.4 Population

Lors de l'utilisation privée de moyens TIC, les utilisateurs (consommateurs) sont globalement responsables de leur sécurité. En général, ils déploient les outils de sécurité couramment disponibles sur le marché (p. ex. antivirus, pare-feu, chiffrage des réseaux sans fil).

Les mesures pour l'amélioration générale de la sécurité des moyens TIC privés ainsi que les offres pour la formation et l'information individuelles ne sont pas coordonnées et ne se fondent pas sur des normes de sécurité communes. Une part toujours plus importante de la population travaille, dans le cadre de son activité, sur des ordinateurs au sein d'entreprises privées ou dans l'administration publique où elle a accès à des données particulièrement sensibles. Pour réduire les risques, il est donc nécessaire que tous les utilisateurs soient formés en conséquence et adoptent des comportements appropriés, comme c'est le cas dans d'autres domaines concernés par les activités de prévention.

3.5 Coopération internationale

La Direction politique du DFAE favorise les contacts internationaux entre la Suisse et les Etats et les organisations internationales qui sont confrontés à la menace dans le cyberespace et crée ainsi les conditions permettant à la Suisse de coopérer au niveau international.

La Direction du droit international public du Département fédéral des affaires étrangères suit les développements internationaux en matière de droit international public, notamment les affaires mêlant l'engagement de moyens cybernétiques lors de conflits interétatiques et le droit humanitaire.

Plusieurs initiatives tentent actuellement d'élaborer des règles internationales. Ces réglementations devraient permettre d'institutionnaliser l'échange d'information permanent sur les technologies, les mesures de protection, le développement des risques et les acteurs. Cela devrait également conduire à un renforcement de l'entraide administrative et judiciaire, et permettre de développer et de mettre en place des mesures communes de sécurité.

Dans le cadre de l'application des résultats du Sommet mondial de l'ONU sur la société de l'information, l'International Telecommunication Union (UIT)[12] a repris la supervision des travaux à l'échelle internationale dans le domaine de la cybersécurité et établi une feuille de route sur ses activités et objectifs. La Suisse participe à ces travaux.

Ces dernières années, de nombreux pays (notamment l'Allemagne, la France et les Pays-Bas) ont adopté des cyberstratégies globales alors qu'ils ne s'étaient jusque là engagés que dans des activités et sujets bilatéraux et multilatéraux choisis. Entre-temps, certains Etats utilisent isolément un large éventail de moyens pour se protéger contre les cyberrisques (p. ex. stratégies nationales, mesures et centres de défense avec structures de commandement). Il serait indiqué de procéder périodiquement à une comparaison de la présente stratégie avec les stratégies susmentionnées. Et ce tout particulièrement parce que la Suisse choisit une démarche qui ne tente pas simplement de résoudre, au sein de processus d'affaires, de production et de gestion, les lacunes en matière de perception de la présence dans le cyberespace et le manque de collaboration opérative en créant une plateforme de coordination centralisée ; elle s'efforce de le faire au sein même des organes et structures compétents et responsables, à tous les échelons.

3.6 Bases juridiques

Une multitude de lois et d'ordonnances contiennent actuellement des bases juridiques concernant le cyberespace, conséquence logique de la mise en réseau et de l'emploi croissants de moyens de communication qui entraînent une présence de plus en plus marquée dans le cyberespace de tâches et de responsabilités apparaissant dans les lois et ordonnances correspondantes. La situation est cependant compliquée, car ces réglementations sont mal coordonnées et présentent, pour certaines, encore des lacunes.

Les prescriptions pour la sûreté de l'information de l'administration fédérale et de l'armée ont été rassemblées par le Conseil fédéral dans l'ordonnance concernant la protection des

[12] Pour en savoir davantage sur les activités de l'UIT dans le domaine de la cybersécurité : http://www.itu.int/cybersecurity/

informations (OPRL)[13], valable jusqu'au 31 décembre 2014. Le rôle des services du Parlement, des tribunaux fédéraux, du Ministère public de la Confédération et des offices cantonaux qui reçoivent des informations de la Confédération n'y sont que peu ou pas traités.

La sécurité informatique de l'administration fédérale n'est réglée que sommairement dans l'ordonnance sur l'informatique dans l'administration fédérale (OIAF)[14]. La plupart des principes et directives en matière de sécurité ne se retrouvent qu'au niveau de directives (directives du 27 septembre 2004 du Conseil de l'informatique de la Confédération concernant la sécurité informatique dans l'administration fédérale[15]).

La loi fédérale sur la protection des données (LPD)[16] et l'ordonnance relative à la loi fédérale sur la protection des données (OLPD)[17] contiennent des exigences minimales générales en matière de sécurité des données dans le cadre de la gestion de données personnelles. Ces exigences sont valables au sein de la Confédération et s'appliquent aussi aux acteurs du secteur privé.

La loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI)[18], qui traite en particulier des mesures pour détecter et combattre le terrorisme, le service de renseignement prohibé, l'extrémisme violent et la violence lors de manifestations sportives, contribue aussi, avec les contrôles de sécurité relatifs aux personnes, à la sécurité de l'information au sein des autorités fédérales.

La loi fédérale sur le renseignement civil (LFRC)[19] règle partiellement les tâches dévolues au renseignement civil de la Confédération, notamment l'acquisition d'informations importantes pour la politique de sécurité concernant l'étranger et leur évaluation à l'intention des départements et du Conseil fédéral, de même que la prise en charge des tâches de renseignement dans le domaine de la sûreté intérieure.

La loi sur l'armée (LAAM, en particulier les art. 99 et 100)[20] et l'ordonnance concernant le Service de renseignement de l'armée (OSRA, en particulier les art. 4 à 6)[21] font office, entre autres, de documents de référence pour tout ce qui concerne les relations à entretenir avec d'autres services de renseignement militaire actifs dans le domaine des cyberrisques. Ils constituent, en outre, la base légale pour le domaine Prévention et intervention de l'unité organisationnelle Autoprotection de l'armée qui est en cours de développement.

Par décision du 12 mai 2010, le Conseil fédéral a chargé le DDPS d'élaborer des bases légales formelles pour la protection et la sécurité de l'information, qui devraient être prochainement uniformisée dans le cadre d'une loi spécifique. Cette loi servira non seulement à protéger la confidentialité des informations, mais aussi leur intégrité, leur

---

13 RS 510.411 Ordonnance du 4 juillet 2007 concernant la protection des informations de la Confédération.

14 RS 172.010.58 Ordonnance du 9 décembre 2011 sur l'informatique et la télécommunication dans l'administration fédérale.

15 Directives du 27 septembre 2004 du Conseil de l'informatique de la Confédération concernant la sécurité informatique dans l'administration fédérale (état au 1er novembre 2007).

16 Loi fédérale du 19 juin 1992 sur la protection des données (LPD ; RS 235.1 ; état au 1er janvier 2011).

17 Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD ; RS 235.11 ; état au 1er décembre 2010).

18 RS 120 Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure.

19 Loi fédérale du 3 octobre 2008 sur le renseignement civil (LFRC ; RS 121 ; état au 1er janvier 2010).

20 RS 510.10 Loi fédérale du 3 février 1995 sur l'armée et l'administration militaire (loi sur l'armée ; LAAM), état au 01.01.2011.

21 RS 510.291 Ordonnance du 4 décembre 2009 concernant le Service de renseignement de l'armée (OSRA), état au 01.01.2010.

disponibilité et leur traçabilité et à assurer la sécurité des moyens permettant de traiter ces informations.

Avec les ordonnances, prescriptions et directives d'exécution, la loi sur les télécommunications (LTC)[22] garantit que la population et l'économie disposent d'une offre de télécommunications variée, à un prix abordable, de haute qualité et compétitive sur le plan national et international. Selon l'article concerné de la LTC, le service universel doit être « sûr ». Des exigences impératives de qualité sont posées au service universel dans l'ordonnance sur les services de communication (OST)[23] et les prescriptions concernées de l'OFCOM. En outre, la LTC doit « assurer que le trafic des télécommunications ne soit pas perturbé et qu'il respecte les droits de la personnalité et les droits immatériels ».

Dans la LTC, comme dans l'OST, un chapitre consacré aux « intérêts nationaux importants » traite de diverses dispositions essentielles du point de vue de la sécurité et sur lesquelles l'OFCOM s'est fondé pour promulguer des directives recommandant des mesures de sécurité et de disponibilité pour les infrastructures et services de télécommunications.

S'agissant en particulier de la sécurité des télécommunications, les prescriptions légales n'exigent un fonctionnement irréprochable des installations que sur le plan technique. La LTC prévoit « la sécurité et la disponibilité des infrastructures et services de télécommunications ». La fiabilité et l'absence d'interférence sont également réglées dans cette loi ainsi que dans d'autres ordonnances. Cependant, la manière dont la sécurité des services de télécommunication et des TIC doit être assurée contre les risques extérieurs et les événements naturels n'est définie dans aucune base légale[24].

La loi sur l'approvisionnement du pays (LAP)[25] et les ordonnances qui en découlent[26,] règlent les mesures préventives de la défense économique du pays et les dispositions garantissant l'approvisionnement du pays en biens et services vitaux en cas de pénuries importantes auxquelles l'économie n'arriverait pas à faire face à elle seule. Un domaine spécifique est en charge des infrastructures de l'information (p. ex. sécurité et transmission des données) et des télécommunications avec l'étranger. Actuellement, un projet de révision complète de la loi sur l'approvisionnement du pays est en cours d'élaboration. La nouvelle orientation prévoit le passage d'une logique de sécurité à une logique des risques, une augmentation de la capacité de résistance de branches vitales de l'économie et le transfert des priorités des biens aux prestations.

La loi sur la surveillance de la correspondance par poste et télécommunication (LSCPT)[27] et le code de procédure pénal (CPP)[28] autorisent, en cas de présomption urgente de culpabilité, l'examen du courrier et des télécommunications, y compris des courriels. Un

---

22 Loi du 30 avril 1997 sur les télécommunications (RS 784.10 ; état au 1er juillet 2010).

23 Ordonnance du 9 mars 2007 sur les service de télécommunication (OST ; RS 784.101.1 ; état au 1er mars 2012).

24 Crisis and Risk Network (CRN), Center for Security Studies (CSS) (2011) : « Die rechtlichen Grundlagen zum Schutz Kritischer Infrastrukturen in der Schweiz » (en élaboration sur mandat de l'OFPP).

25 Loi fédérale du 8 octobre 1982 sur l'approvisionnement économique du pays (LAP ; RS 531 ; état au 1er janvier 2011).

26 Ordonnance du 6 juillet 1983 sur l'organisation de l'approvisionnement économique du pays (ordonnance d'organisation de l'approvisionnement du pays ; RS 531.11 ; état au 6 juillet 2003) ; ordonnance du 2 juillet 2003 sur les préparatifs en matière d'approvisionnement économique du pays (RS 531.12 ; état au 2 juillet 2003).

27 Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT ; RS 780.1 ; état au 1er janvier 2011).

28 RS 312.0 Code de procédure pénale suisse du 5 octobre 2007.

recensement rétroactif de données de facturation et de données relatives au trafic des communications ainsi qu'une identification des participants sont, en outre, autorisés par la loi.

La convention du Conseil de l'Europe sur la cybercriminalité, qui est entrée en vigueur le 1er janvier 2012 en Suisse, engage les Etats signataires à sanctionner les escroqueries informatiques, le vol de données, la falsification de documents ou l'intrusion dans un système informatique protégé. La convention règle la manière dont les preuves sont relevées et sauvegardées sous forme de données électroniques au cours de l'enquête pénale. Les enquêteurs doivent pouvoir accéder rapidement aux données traitées électroniquement pour que celles-ci ne soient pas falsifiées ou détruites en cours de procédure. Le Code pénal suisse et ses normes, notamment les prescriptions en matière de droit pénal concernant l'informatique dans le Code pénal suisse (CP)[29], en particulier les articles 143, 144bis, et 272 à 274, peuvent être appliqués à des cas de cybercriminalité. La convention du Conseil de l'Europe règle aussi la collaboration internationale entre Etats concernant des affaires pénales (p. ex. entraide judiciaire et extradition). La collaboration entre les différents Etats doit se dérouler rapidement et efficacement.

3.7 Bilan

L'analyse des structures en place montre que les milieux économiques (spécialement les fournisseurs de prestations TIC et les fournisseurs de systèmes importants) ainsi que les autorités fédérales et cantonales disposent de nombreuses capacités permettant de mesurer l'ancrage de leurs missions et responsabilités dans le cyberespace et d'identifier ainsi les risques y afférents. Il existe aussi des démarches et des concepts d'amélioration de la situation en matière de cybersécurité et des organes qui assurent un échange d'informations entre certains acteurs et assument une fonction de coordination. De grandes entreprises, des corps cantonaux de police et des unités administratives de la Confédération disposent de services qui ont des connaissances spécialisées de pointe. Divers instituts suisses de recherche travaillent également sur des projets dans le domaine de la cybersécurité et plus précisément dans celui de l'identification et de l'évaluation des cyberrisques. Souvent, les processus n'intègrent pas tous les décideurs, du niveau technico-opératif au niveau politico-stratégique, ou alors ceux-ci décident consciemment de ne pas y prendre part.

Il ressort cependant de l'enquête menée auprès de représentants de l'économie et d'opérateurs d'infrastructures critiques, qu'il reste à surmonter d'importantes lacunes et faiblesses face aux cyberattaques. Ainsi, les capacités et les perceptions aux différents niveaux susmentionnés sont de nature et de qualité très diverses, souvent insuffisantes ; elles ne sont, en outre, que partiellement coordonnées et, pour une grande partie, déterminées par des intérêts économiques. Les mesures prises ou prévues pour améliorer la cybersécurité sont l'expression d'une perception très diverse et donc hétérogène des risques. Elles conduisent à des actions non coordonnées et l'échange d'informations entre les acteurs fonctionne difficilement ou se limite souvent à des échanges internes à un domaine ou une entreprise.

Les lacunes enregistrées au niveau de la cybersécurité sont souvent dues à un manque de ressources humaines et financières. Ce constat, s'il vaut pour l'économie, s'applique surtout pour la Confédération dont les ressources humaines sont insuffisantes, à tel point qu'en

[29] RS 311.0 Code pénal suisse du 31 décembre 1937.

situation normale déjà, les missions de bases ne peuvent être que partiellement accomplies. Ceci résulte aussi de la pénurie avérée de spécialistes en TIC.

En matière de collaboration entre l'économie et les autorités, on constate diverses faiblesses et un besoin de clarification, s'agissant de la répartition des tâches, des capacités et des compétences. L'analyse des structures existantes a tout particulièrement mis en lumière un manque, au sein de l'administration fédérale, de moyens suffisants pour identifier les risques, évaluer globalement les informations et apprécier les situations au profit de l'économie, des opérateurs d'infrastructures critiques et des autorités ; le niveau de protection contre les cyberrisques ne peut donc être qu'insuffisant en raison d'un déficit en matière d'échange d'informations. Par ailleurs, la collaboration avec deux types d'acteurs sensibles, les fournisseurs de prestations TIC et les fournisseurs de systèmes, est encore trop peu systématisée. En outre, les synergies entre organes des autorités devraient être mieux exploitées et les systèmes et moyens d'annonce devraient être analysés à l'aune de leur efficience tout en tenant compte de l'aspect de l'échange d'informations. Des analyses des risques et des définitions qui en découlent pour les exigences en matière de sécurité des infrastructures TIC, de même qu'une répartition des responsabilités et des surcoûts, font aussi défaut.

Internet est encore trop souvent considéré comme une zone de non-droit par de très nombreux acteurs et la sécurité quotidienne liée à son utilisation n'est qu'insuffisamment assurée. Les autorités de poursuite pénale en particulier ne disposent pas toujours de moyens et de capacités en suffisance pour sanctionner efficacement les infractions. En outre, il reste encore des zones d'ombre en ce qui concerne les interfaces et l'échange d'informations avec des organes assumant un rôle de prévention dans le contexte de la réduction des cyberrisques pour parvenir à une combinaison productive de mesures préventives et répressives.

On constate globalement que le système en place permet à peine d'identifier à temps des cyberattaques ciblées de grande ampleur, de se défendre activement contre elles et d'en maîtriser rapidement et efficacement les effets, si ceux-ci sont graves. En conséquence, les entreprises et les opérateurs d'infrastructures critiques qui ont répondu à l'enquête réclament que des prescriptions de sécurité minimales soient édictées conjointement avec les autorités, puis mises en œuvre. De même, ils souhaitent une meilleure coordination des mesures permettant d'améliorer la situation sur le plan de la sécurité, la maîtrise des attaques et la sensibilisation. La Confédération est aussi fortement sollicitée à institutionnaliser l'échange d'informations, rendre disponible une image mise à jour de la cybersituation et garantir un appui subsidiaire renforcé.

Les diverses bases juridiques existantes reflètent l'ancrage des tâches et des responsabilités dans le cyberespace. Par conséquent, opter pour une loi unique dédiée spécialement au cyberespace serait inapproprié. La législation existante doit donc être adaptée en permanence aux développements de tout domaine d'application dans le cyberespace et faire l'objet de révisions.

On constate également un accroissement du réseau et de la collaboration à l'échelon international en vue de réduire les cyberrisques.

Se fondant sur cette nécessité patente d'agir, la présente stratégie propose une série de mesures concrètes, présentées ci-après.

4 DISPOSITIF DE PROTECTION CONTRE LES CYBERRISQUES

4.1 Objectifs prioritaires

Le Conseil fédéral admet que la problématique de la cybernétique est avant tout liée à son influence sur des tâches et des responsabilités existantes incombant aux autorités, à l'économie et à la société. La limitation des cyberrisques est donc l'affaire des responsables concernés.

Le Conseil fédéral entend favoriser le cyberespace dans la mesure où il offre des avantages et des chances à l'économie, au monde politique et à la population de la Suisse. Il constate cependant que les développements dans ce domaine impliquent également des risques et que des mesures limitatives idoines sont nécessaires.

La présente stratégie nationale règle l'application en temps de paix des mesures décrites et exclut donc explicitement les situations de guerre.

Le Conseil fédéral poursuit, à travers la stratégie nationale de protection de la Suisse contre les cyberrisques, les objectifs prioritaires ci-après.

- Les cyberrisques doivent être décelés et évalués suffisamment tôt pour que des mesures préventives de limitation des risques puissent être prises en collaboration avec tous les acteurs concernés de l'économie, du monde politique et de la société.
- La capacité de résistance (résilience) des infrastructures critiques face aux cyberattaques - c'est-à-dire leur capacité à rétablir la situation le plus rapidement possible - doit être accrue, en collaboration avec leurs opérateurs, les fournisseurs de prestations TIC et les fournisseurs de systèmes et les responsables du programme de la Confédération pour la protection des infrastructures critiques (programme PIC).
- Les conditions permettant d'affronter efficacement les cyberrisques – en particulier la cybercriminalité, le cyberespionnage et le cybersabotage – doivent être assurées, voire créées si nécessaire.

Ces objectifs peuvent être atteints de diverses manières au sein des structures décentralisées existantes. Dans tous les cas, la *responsabilité individuelle* dans les divers domaines économiques, ainsi que le *dialogue* et la *collaboration* entre les secteurs de l'économie et les autorités, constituent les conditions essentielles pour y parvenir. L'*échange* permanent *d'informations* doit assurer la *transparence* et la *confiance*, et l'Etat doit restreindre ses interventions aux cas où l'intérêt public est en jeu et agir en accord avec le principe de *subsidiarité.*

Le traitement des cyberrisques est une tâche transversale que les milieux économiques, les opérateurs d'infrastructures critiques, les fournisseurs de prestations TIC, les fournisseurs de systèmes et les autorités doivent assumer, tant au niveau cantonal que fédéral*.* Ceux-ci doivent être perçus comme faisant partie intégrante d'un processus intégral d'affaires, de production ou d'administration*.* Dans ces processus, tous les acteurs, du niveau techno-administratif au niveau politico-stratégique, doivent être impliqués*.* Une approche efficace des dangers et des menaces émanant d'Internet présuppose la prise de conscience du fait que les tâches et les responsabilités dévolues aux autorités, aux milieux économiques et à la population laissent des traces dans le cyberespace*.* Chaque unité organisationnelle des milieux politiques, de l'économie et de la société est responsable de reconnaître les conséquences de ses activités dans le cyberespace, d'intégrer les risques qui en découlent dans ses processus afin de les réduire*.* A cette fin, les structures décentralisées existantes

doivent être dotées des compétences nécessaires ou de capacités renforcées pour pouvoir assumer entièrement la part spécifiquement cybernétique de leurs tâches et de leurs responsabilités.

4.2 Conditions générales et prérequis

Bases juridiques

Etant donné que la problématique de la cybernétique touche les tâches et responsabilités existantes, il est nécessaire, dans un premier temps, de vérifier si les bases juridiques en vigueur en tiennent compte. Au besoin, les dispositions nécessaires doivent être intégrées en priorité dans les lois en vigueur et dans celles prévues (p. ex. la loi sur les services de renseignement). Le besoin de réglementation qu'exige le cyberespace doit donc être étroitement coordonné avec les projets législatifs en cours ou prévus (p. ex. la législation sur la sûreté de l'information, la loi sur les services de renseignement, la loi sur l'approvisionnement du pays, la loi fédérale sur la surveillance de la correspondance, la convention sur la cybercriminalité, etc.)

L'adaptation des bases juridiques au développement rapide du cyberespace et des cyberrisques est un processus permanent. Au besoin, des expertises juridiques doivent être réalisées pour répondre aux questions complexes. Les bases juridiques sur lesquelles se fondent les autorités de poursuite pénale (en particulier le code pénal, le code de procédure pénale, les lois cantonales de police et la réglementation des compétences) et des unités actives dans le domaine préventif (Service de renseignement de la Confédération et corps cantonaux de police) doivent être contrôlées à la lumière des conditions particulières du cyberespace (p. ex. les distances géographiques, la rapidité et la fugacité des traces et ainsi l'utilisation des indices dans le domaine de la justice). Il s'agit surtout de déterminer comment des actes commis au moyen de réseaux électroniques peuvent être identifiés et empêchés à temps, et comment des enquêtes peuvent être menées efficacement à leur sujet. La pesée des intérêts entre la protection de la personnalité et la sûreté publique et intérieure doit faire l'objet d'une attention particulière.

Il s'agit également de reconsidérer les responsabilités des opérateurs de systèmes et réseaux informatiques, des fournisseurs d'infrastructures TIC (réseau) et des prestataires de service ou de tout autre acteur présent sur Internet. Ici également, il y a lieu de procéder à une pesée des intérêts au niveau juridique et politique entre l'obligation de protection des données et le droit de toutes les parties de traiter des données afin de permettre les coopérations visant la protection les infrastructures TIC ainsi que celle des personnes, tant privées que publiques.

Echange d'informations et prévention

L'impact de la cybernétique sur les tâches et les responsabilités, et donc les risques qui en découlent, doivent être reconnus et analysés. Cette tâche incombe à chaque autorité dans le cadre d'échanges avec les acteurs de l'économie et de la société. L'étroite collaboration entre les acteurs privés et publics sous forme de *partenariat public-privé (PPP)* a été jugée productive par le Conseil fédéral en 2003 et 2007 et doit être poursuivie[30].

Pour brosser un tableau complet de la situation, des informations – qu'elles soient techniques ou non – doivent être accumulées de façon coordonnée, analysées et évaluées. Les résultats des investigations sont ensuite mis à la disposition de tous les acteurs. Il est

[30] Cf. ACF 2003 et 2007

dès lors important de resserrer plus fortement, dans le cadre de MELANI, les liens existant entre les capacités propres aux services de renseignement et les capacités techniques, en faveur des exploitants d'infrastructures critiques et de l'économie.

On attend de l'Etat qu'il dispose de moyens lui permettant d'appuyer subsidiairement des entités responsables lorsque celles-ci ne sont plus capables de prendre elles-mêmes des mesures leur permettant de venir à bout de la situation.

Collaboration avec l'étranger

Les cyberrisques ne connaissent pas de frontières. Pour une analyse pertinente et réaliste de ces risques, la coopération internationale est essentielle. Le partage des expériences, des travaux de recherche ou de développement, des informations sur certains incidents ainsi que des résultats sur les activités en rapport avec l'instruction et les exercices doit donc être renforcé.

Les efforts consentis dans l'établissement de règles et de normes internationales en vue de préserver le cyberespace de tout abus sont dans l'intérêt d'un pays technologiquement très développé comme la Suisse. Notre pays participe donc, dans le cadre d'organisations internationales étatiques et non étatiques, à la recherche de solutions au niveau politique, de possibilités de coopération et de conventions de droit international public visant à réduire les cyberrisques. Les problèmes liés à la structure de l'interconnexion numérique mondiale ainsi que la création et l'influence de normes et règles internationales sont, idéalement, abordés dans le cadre de forums mondiaux. C'est pourquoi les intérêts suisses du monde de l'économie, des autorités et de la société doivent être exposés à ce niveau déjà.

Il en va de même de la mise en place de coopérations pour la gestion conjointe des crises. Une collaboration renforcée en matière de services de renseignement, d'échange d'informations avec les fournisseurs de prestations TIC et fournisseurs de systèmes concernés, d'analyse technique et de poursuite pénale (entraide administrative et judiciaire) contribue à augmenter la liberté de manœuvre et l'efficacité des mesures prises par la Suisse, en y incorporant également les acteurs non étatiques. Dans ce contexte, l'implication aux différents niveaux d'acteurs tels que les associations professionnelles, les groupes d'intérêts, les groupes internationaux de travail ou les organisations non gouvernementales, est aussi nécessaire.

Poursuite pénale

Des informations utilisables dans le cadre des procédures judiciaires doivent être collectées sur les activités criminelles perpétrées dans le cyberespace, leurs auteurs poursuivis et les infractions punies. De même, la collaboration avec les autorités étrangères de poursuite pénale doit être assurée. La priorité stratégique en matière de criminalité fixée par le Conseil fédéral pour la période s'étendant de 2012 à 2015 exige également des autorités de poursuite pénale qu'elles se concentrent sur les cyberattaques, qui sont considérées tant comme des délits graves contre la protection de l'Etat que comme une forme particulière de la criminalité économique.

Armée

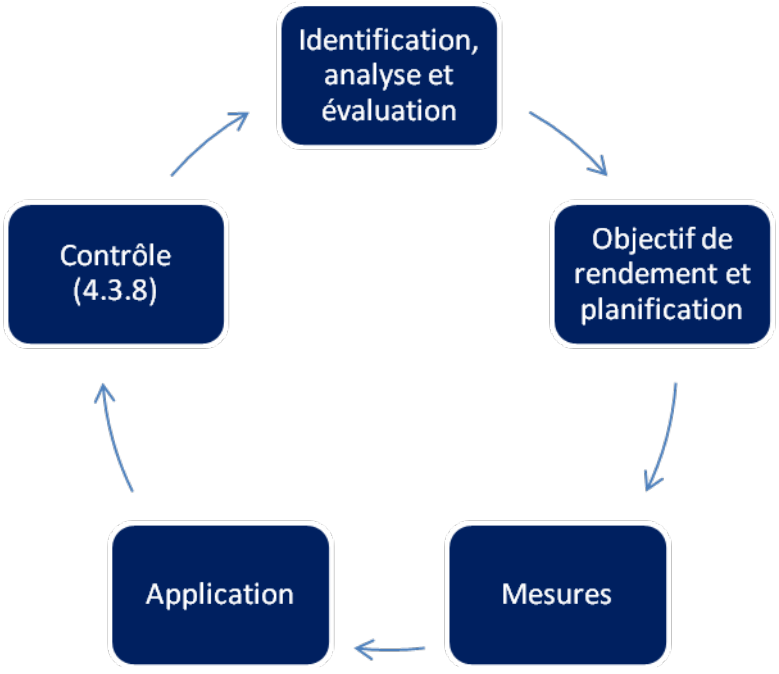
L'armée, en tant que réserve stratégique de la Suisse, doit pouvoir accomplir ses missions, quelles que soient les formes de son engagement. Elle prend, dès lors, des mesures pour protéger ses propres infrastructures et assure la conduite en cas de crise avec des moyens infrastructurels capables de résister à toute défaillance, lesquels peuvent, sur demande, être mis à disposition d'autres autorités ou opérateurs d'infrastructures en cas de nécessité. Il en va de même pour les enseignements tirés des activités de l'armée.

Dans ce sens, l'armée est étroitement liée au domaine civil et doit, dans le cadre du développement de ses capacités à réduire les cyberrisques, harmoniser la phase de concrétisation avec les autres autorités.

4.3 Champs d'action et mesures

Dans le cadre de l'application des mesures visant une meilleure protection de la Suisse contre les cyberrisques, il s'agit de prendre en compte les notions d'utilité politique et économique, de proportionnalité et d'efficacité et de tenir compte de l'aspect décentralisé de l'infrastructure étatique et économique de la Suisse. Cela implique pour tous les acteurs d'établir dans quelle mesure leurs tâches et responsabilités ont des implications dans le cyberespace et avec quels partenaires économiques, politiques et sociaux ils doivent engager des mesures visant à réduire les risques.

Ce processus effectué, des champs d'action et des mesures devant permettre de réduire les cyberrisques sont définis. Ces champs d'action sont décrits tout au long d'un cycle de gestion des risques et de protection[31]. Durant ce cycle, qui comprend cinq processus partiels (identification, analyse et évaluation ; objectif de rendement et planification ; mesures ; application ; contrôle), la présente stratégie ne s'applique, pour chacun des champs d'action, que lors des trois premières étapes (identification, analyse et évaluation ; objectif de rendement et planification ; mesures).



L'application des mesures est du ressort des acteurs compétents de l'administration, de l'économie et de la société. Dans la mesure où les étapes de l'application concernent des organes fédéraux, celles-ci sont décrites. Il s'agit tout d'abord des premières étapes de mise en œuvre à l'échelon de la Confédération en vue de lancer la planification de l'application à

[31] Le cycle de gestion des risques et de protection prend fortement appui sur le cycle de protection mis en place dans le cadre de la stratégie nationale pour la protection des infrastructures critiques (à l'OFPP) et appliqué au niveau de l'approvisionnement économique du pays.

tous les niveaux, en collaboration avec les partenaires concernés de l'administration, de l'économie et de la société.

Quant au contrôle des mesures appliquées, il incombe à l'organe de coordination devant être créé et agissant en étroite collaboration avec les organes responsables.

4.3.1 Champ d'action 1 : recherche et développement

Identification, analyse et évaluation

Les nouveaux risques en lien avec la problématique de la cybernétique doivent être étudiés pour que les milieux de la politique, de l'économie et de la recherche puissent être informés et prendre des décisions à temps. Le domaine de la recherche focalise ses activités en fonction des tendances technologiques, sociales, politiques et économiques pouvant avoir un impact sur les cyberrisques. Les processus de recherche et de développement sont lancés, voire exécutés, par les acteurs des domaines des sciences, de l'économie, de la société et des autorités.

Objectifs de rendement et planification

Il est indispensable que chaque secteur de responsabilité ait les capacités d'identifier d'évaluer et d'analyser les risques en lien avec la problématique de la cybernétique. Ce processus doit s'effectuer en collaboration avec les responsables de la stratégie du Conseil fédéral pour une société de l'information en Suisse (DETEC-OFCOM), de la stratégie nationale pour la protection des infrastructures critiques (DDPS-OFPP) ainsi que de la gestion des risques de la Confédération.

Mesures

Mesure 1

Les organes fédéraux responsables s'informent mutuellement de l'état de la situation et des développements liés aux cyberrisques. Ils intègrent également à leurs échanges des acteurs extérieurs à l'administration fédérale et procèdent, au besoin, à des recherches *intra muros* ou confient des mandats de recherche à l'externe.

Application

Les organes fédéraux sont responsables de la recherche sectorielle dans leurs propres domaines de compétences. Le comité de pilotage Formation, Recherche et Technologie (comité de pilotage FRT) charge les offices de traiter les programmes pluriannuels préparés sur la recherche sectorielle dans leurs domaines politiques (concepts de recherche). Ces concepts renseignent sur les points forts prévus dans le cadre de la recherche sectorielle. Ils tiennent notamment compte des éléments-clés relevés par les hautes écoles dans leurs recherches, des programmes réalisés par le FNS sur mandat de la Confédération et des activités de la CTI.

4.3.2 Champ d'action 2 : analyse des risques et vulnérabilités

Identification, analyse et évaluation

Les organes compétents des autorités, les opérateurs d'infrastructures critiques, les fournisseurs de prestations TIC et les fournisseurs de systèmes ainsi que les associations

(au sens d'un regroupement de branches) doivent identifier, à leur niveau, les risques liés au cyberespace ; de même, ils doivent évaluer et analyser leur probabilité d'occurrence et leurs effets potentiels.

Objectifs de rendement et planification

Les acteurs responsables du monde politique, de l'économie et de la société doivent disposer des moyens et des capacités leur permettant d'identifier à temps les cyberrisques, de jauger la menace et d'étudier les implications pour leur domaine par des analyses communes des risques. Ce processus se concrétise dans le cadre d'une collaboration avec les responsables de la gestion des risques de la Confédération, de la « stratégie nationale pour la protection des infrastructures critiques » et des travaux menés dans le cadre de l'analyse nationale des dangers « Risques suisses ».

Mesures

Mesure 2

Les analyses des risques et des vulnérabilités doivent être menées à tous les niveaux (Confédération, cantons et opérateurs d'infrastructures critiques) en impliquant les fournisseurs de prestations TIC et les fournisseurs de systèmes. Elles comprennent le contrôle régulier et indépendant des systèmes par les opérateurs. La mise au point d'analyses (sectorielles) de risques exige une collaboration étroite avec les autorités. **(DFE, DFF, DETEC)**

Application

Le DFE, dans le cadre de la révision de la LAP[32] , adapte ses compétences pour pouvoir analyser, en fonction des besoins, les risques et les vulnérabilités avec tous les secteurs partiels de l'approvisionnement économique du pays (OFAE), en impliquant, selon la situation, les autorités compétentes (avant tout celles du DETEC et du DFF). Si certains exploitants d'infrastructures critiques ne sont pas recensés par l'AEP, ils doivent être abordés par les autorités compétentes qui adapteront, au besoin, la législation dans leurs secteurs spécifiques. Les analyses des risques et des vulnérabilités doivent être menées selon une procédure aussi standardisée que possible. Les autorités compétentes (avant tout celles du DETEC et du DFF) doivent être impliquées lors de la mise en œuvre des résultats.

Les résultats étayant l'analyse globale de la menace sont consolidés dans le cadre d'une collaboration avec MELANI.

Mesure 3

Les autorités, les exploitants d'infrastructures critiques et les instituts de recherche examinent, en impliquant les fournisseurs de prestations TIC et les fournisseurs de systèmes, leurs infrastructures TIC sous l'angle de leurs vulnérabilités, notamment de leurs faiblesses systémiques, organisationnelles et techniques. Les résultats sont consolidés et

[32] RS 531 Loi fédérale du 8 octobre 1982 sur l'approvisionnement économique du pays

évalués, voire publiés dans des rapports spécifiques s'ils présentent un intérêt public[33]. **(DFE, DFF, DDPS, DETEC)**

Application
L'unité de pilotage informatique de la Confédération (UPIC) – organe du DFF – élabore pour la mi-2013, en collaboration avec les fournisseurs de prestations TIC, un concept de contrôle périodique des infrastructures TIC de l'administration fédérale au niveau des faiblesses systémiques, organisationnelles et techniques. Ce concept sera appliqué par les fournisseurs de prestations compétents et les responsables concernés des secrétariats généraux des départements.
Le concept de contrôle peut servir de recommandation ou d'appui au secteur de l'économie et aux exploitants d'infrastructures critiques dans le cadre de leurs propres contrôles.

Les résultats étayant l'analyse globale de la menace sont consolidés dans le cadre d'une collaboration avec MELANI.

4.3.3 Champ d'action 3 : analyse de la menace

Identification, analyse et évaluation
Les incidents d'importance nationale ou particulière doivent être identifiés, évalués et analysés. Le traitement et la mise à disposition des résultats de cette procédure doivent être adaptés aux secteurs de responsabilité et mis à leur disposition.

Objectifs de rendement et planification des prestations
Les acteurs du monde politique, de l'économie et de la société doivent disposer des moyens et des capacités leur permettant d'identifier, d'évaluer et d'analyser les menaces, en étroite collaboration avec les responsables. Au besoin, la possibilité d'octroyer une autorisation d'annoncer aux organes, aux opérateurs d'infrastructures critiques et aux acteurs de l'économie responsables doit être examinée.

Mesures

Mesure 4
Des informations en matière de renseignement, policières, forensiques ou techniques, provenant de sources publiques ou non, sur les menaces et les risques dans le cyberespace sont acquises, évaluées et analysées. Les résultats qui en découlent doivent être rassemblés dans le cadre du modèle PPP de MELANI, évalués globalement, analysés et condensés dans une présentation et un suivi de la situation, de même que combinés à des scénarios envisageant des possibilités d'évolution de la situation. Ces résultats sont mis à la disposition des acteurs responsables concernés. **(DFF, DDPS)**

Application
Le Service de renseignement de la Confédération devra assumer les aspects cybernétiques de son mandat pour maîtriser et assurer le suivi des cas intéressant la protection de l'Etat en lien avec les moyens TIC. Ce processus implique la BAC comme fournisseur technique de

[33] Les méthodes et les produits cryptographiques permettant de protéger les informations classifiées (CONFIDENTIEL / SECRET) doivent, selon l'ordonnance concernant la protection des informations, être autorisées par le service de cryptologie du DDPS.

prestations pour le SRC et, si cela s'avère indiqué, le RM. Les résultats viennent, par l'entremise de la centrale MELANI, étayer l'analyse globale de la menace.

Les capacités techniques permettant de surveiller constamment (24h/24, 7j/7) les réseaux de la Confédération doivent être développés auprès des fournisseurs de prestations (CERT) d'ici à fin 2015. Les résultats viennent, par l'entremise de la centrale MELANI, étayer l'analyse globale de la menace.

La centrale intensifie l'échange volontaire d'informations avec les opérateurs d'infrastructures critiques et ses partenaires internationaux. Cela accroît le besoin en capacités forensiques, augmente le flux d'informations et intensifie l'échange d'informations avec les opérateurs d'infrastructures critiques et le monde économique. Des capacités supplémentaires sont créées dans le cadre d'une collaboration systématique avec les fournisseurs de prestations TIC et fournisseurs de systèmes concernés.

Mesure 5

La Confédération, les cantons et les opérateurs d'infrastructures critiques doivent assurer un suivi des incidents importants et étudier les possibilités de développer leurs propres mesures face aux incidents ayant un rapport avec les cyberrisques. En principe, cette procédure est individuelle et se déroule dans le cadre du mandat de chacun. Les résultats obtenus doivent être rassemblés dans le cadre du modèle PPP de MELANI, évalués globalement, analysés et mis à la disposition des acteurs concernés, en particulier ceux qui sont compétents pour analyser les risques et les vulnérabilités. **(DFF, DDPS)**

Application

MELANI intensifie l'échange volontaire d'informations entre les opérateurs d'infrastructures critiques, les fournisseurs de prestations TIC et les fournisseurs de systèmes concernés et apporte son soutien dans le cadre du suivi des incidents significatifs. Cela accroît le besoin en capacités forensiques, augmente le flux d'informations et intensifie l'échange d'informations avec les opérateurs d'infrastructures critiques et le monde économique.

Le Service de renseignement de la Confédération devra assumer les aspects cybernétiques de son mandat pour maîtriser et assurer le suivi des cas intéressant la protection de l'Etat en lien avec les moyens TIC. Ce processus implique la BAC comme fournisseur technique de prestations pour le SRC. Les résultats viennent, par l'entremise de la centrale MELANI, étayer l'analyse globale de la menace.

Les capacités techniques permettant de surveiller constamment (24h/24, 7j/7) les réseaux de la Confédération doivent être développés auprès des fournisseurs de prestations (CERT). Les résultats viennent, par l'entremise de la centrale MELANI, étayer l'analyse globale de la menace.

Mesure 6

Il s'agit de garantir une vue d'ensemble aussi large que possible des cas (infractions) au niveau national et de coordonner les cas complexes intercantonaux. Les informations acquises à partir des vues d'ensemble et les résultats sur les cas complexes, et en particulier les informations acquises par l'analyse technico-opérative dans le cadre d'une procédure pénale, doivent être intégrés dans la présentation globale de la situation. **(DFJP)**

Application

Le DFJP élabore d'ici à fin 2016, en collaboration avec les cantons, un concept de gestion offrant une vue d'ensemble globale des cas (infractions). Ce concept porte aussi sur la

clarification d'interfaces avec d'autres acteurs dans le domaine de la réduction des cyberrisques, sur la coordination avec la présentation de la situation et sur les ressources et les adaptations juridiques – tant au niveau de la Confédération qu'à celui des cantons - qui sont nécessaires pour le concrétiser.

Les informations acquises à partir des vues d'ensemble (infractions) et les résultats sur les cas complexes obtenus par l'analyse technico-opérative dans le cadre d'une procédure pénale, sont intégrés par MELANI dans l'analyse globale de la menace.

4.3.4 Champ d'action 4 : formation des compétences

Identification, analyse et évaluation
Tous les acteurs de l'économie, de la société et des autorités doivent être sensibilisés aux cyberrisques et formés pour qu'ils puissent les reconnaître et prendre des mesures qui limiteront leur exposition.

Objectifs de rendement et planification
Pour accroître la prise de conscience face aux cyberrisques et donc la capacité à réagir correctement, des mesures de sensibilisation et de formation doivent être élaborées, en tenant compte des approches et des initiatives existantes, avant d'être appliquées dans les différents secteurs de responsabilité. Ce processus s'effectue en coordination étroite avec la concrétisation de la stratégie du Conseil fédéral pour une société de l'information en Suisse.

Mesures

Mesure 7
Un aperçu des offres existantes en matière de formation des compétences doit être établi dans le but de servir de document de référence permettant non seulement de déceler les offres lacunaires, mais aussi d'informer les acteurs de l'économie, de l'administration et de la société civile des offres relatives au traitement des cyberrisques adaptées à leurs besoins. **(DFF, DETEC, DFAE)**

Application
L'organe de coordination et de concrétisation de la stratégie soutient l'établissement d'un aperçu des offres formelles et informelles de formation en vue de renforcer les compétences dans le cyberespace et identifie les exemples de grande qualité et les offres lacunaires. Ce processus durera jusqu'à fin 2013 et se déroulera en coordination étroite avec les travaux de concrétisation de la stratégie du Conseil fédéral pour une société de l'information en Suisse et les cantons. Le DFAE transmet des informations sur les offres faites dans le cadre d'organisations et d'institutions internationales. Les offres de formation et les exemples de grande qualité seront publiés, sous une forme adéquate, avant la mi-2014.

Mesure 8
Les lacunes reconnues de l'offre de formation des compétences en vue du traitement des cyberrisques doivent être abordées, tout comme le recours accru aux exemples de grande qualité. ***(DFF, DETEC)***

Application
L'organe de coordination et de concrétisation de la stratégie organise, en liaison étroite avec la « stratégie du Conseil fédéral pour une société de l'information en Suisse et les cantons » et l'économie, l'élaboration d'un concept de concrétisation visant un recours accru aux offres existantes d'un niveau de qualité élevé en rapport avec le traitement des cyberrisques et la création de nouvelles offres formelles et informelles de formation des compétences d'ici à la mi-2015. Les offres - par exemples des campagnes ou des guides de formation - concernent tant les échelons administratifs et techniques que stratégiques.

4.3.5 Champ d'action 5 : gouvernance d'Internet et directives internationales

Identification, analyse et évaluation
La gouvernance d'Internet[34] fonctionne selon les principes définis lors du Sommet mondial de l'ONU sur la société de l'information (SMSI), qui s'est tenu à Genève en 2003 et à Tunis en 2005. Ce sont ceux d'une organisation comportant de multiples parties prenantes, c'est-à-dire impliquant plusieurs groupes d'intérêt et autorités agissant dans le cadre de leurs rôles respectifs. Tous les acteurs significatifs et responsables (autorités, économie et société) peuvent s'investir dans ce processus. Les règles d'utilisation et d'administration d'Internet sont fondamentales pour les possibilités, les devoirs et les droits des citoyens, des entreprises et des Etats dans un monde interconnecté, libre et compétitif. En raison du caractère global et divers d'Internet, les réglementations dont il est l'objet ne peuvent être décidées et appliquées unilatéralement par certains Etats que dans une très moindre mesure. Cela vaut également pour la formulation de directives, de bonnes pratiques et la constitution d'organes établissant des normes de sécurité pour les produits et processus.

Les intérêts de petits Etats comme la Suisse, en particulier, ne peuvent être défendus au niveau mondial que par une diplomatie « proactive » et la mise en valeur coordonnée de positions dans le réseau global.

Objectifs de rendement et planification

Les problèmes structurels de l'interconnexion mondiale sont idéalement abordés au niveau mondial. C'est pourquoi les intérêts suisses du monde de l'économie, de la société et des autorités doivent être exposés autant que possible de façon coordonnée.

Les ressources essentielles d'Internet doivent néanmoins continuer d'être administrées selon des principes libéraux, en réduisant cependant la domination des intérêts des quelques pays dont Internet est une industrie. Les lignes directrices communes doivent être fixées et concrétisées en commun par les gouvernements. La stabilité et la disponibilité d'Internet doivent être garanties pour tous et la liberté des citoyens et des entreprises d'agir sur Internet ne peut se voir limitée disproportionnellement.

Dans l'optique de l'élaboration de bonnes pratiques, de directives et de conventions internationales dans le domaine des normes de sûreté et de sécurité, ainsi que dans le contexte de la politique de sécurité, il est nécessaire de faire preuve de coordination, principalement de la part des acteurs économiques et des autorités, pour exposer les intérêts de la Suisse.

[34] Tunis Agenda for the Information Society (WSIS 2005), §34

Mesures

Mesure 9
La Suisse (économie, société, autorités) s'engage activement, et de manière coordonnée, en faveur d'une gouvernance d'Internet qui s'accorde avec la conception que la Suisse se fait de la liberté et de la responsabilité (individuelle), du service universel, de l'égalité des chances, des droits de l'homme et de l'Etat de droit. La Suisse s'engage pour une internationalisation et une démocratisation adéquates de la gestion d'Internet. Son expérience du processus démocratique de prises de décisions lui permet d'apporter une plus-value dans la recherche du consensus. **(DETEC, DFAE, DDPS, DFF)**

Application
Le DETEC représente la Suisse et ses intérêts dans les processus et institutions significatifs dans le domaine de la gouvernance d'Internet. Il coordonne et détermine les intérêts et les positions de la Suisse dans ce domaine avec les organes fédéraux concernés. En outre, il exploite une plate-forme d'échange multipartite (« Plateforme Tripartite ») ouverte à tous les acteurs intéressés de l'administration suisse, de l'économie privée, de la société civile et du monde académique et prend en compte leurs intérêts avec pondération.

La représentation des acteurs concernés dans les instances internationales et les manifestations relevant de la politique de sécurité qui ont une influence, directe ou indirecte, sur la gouvernance d'Internet, est assurée par le DFAE et le DDPS.

Le DETEC et le DFAE établissent pour la fin de 2013, en collaboration avec les départements participants, un aperçu des manifestations et des initiatives prioritaires ainsi que des instances internationales qui ont un lien avec la gouvernance d'Internet.

Mesure 10
La Suisse collabore avec d'autres Etats et des organisations internationales au niveau de la politique internationale de sécurité pour faire face aux menaces émanant du cyberespace. Elle suit l'évolution de la situation dans ce domaine sur la scène diplomatique et favorise les échanges politiques dans le cadre de conférences internationales et d'autres initiatives diplomatiques. **(DFAE, DDPS)**

Application
Le DFAE, en collaboration avec le DDPS, représente la Suisse sur le plan diplomatique et défend les intérêts de la politique de sécurité de notre pays devant les organisations internationales et les autres Etats. Il s'engage en faveur d'initiatives relevant du droit international public qui ont pour but de préserver le cyberespace de tout conflit.

Mesure 11
Les opérateurs, associations et autorités s'organisent dans le cadre d'initiatives, privées ou étatiques, de conférences et de processus de standardisation pour s'impliquer dans ces organes. ***(DETEC, DFAE, DDPS, DFF)***

Application
MELANI et le DETEC intensifient l'échange d'informations entre les opérateurs d'infrastructures critiques, les fournisseurs de prestations TIC, les fournisseurs de systèmes et les associations en ce qui concerne les démarches et les initiatives internationales. Pour ce faire, MELANI et le DETEC soutiennent l'implication coordonnée de la place économique

suisse dans ces organes internationaux et y prennent part, pour autant que cela soit souhaité, en accord avec les départements, le DFAE en particulier.

4.3.6 Champ d'action 6 : gestion de la continuité et des crises

Identification, analyse et évaluation
Les activités des divers acteurs doivent être coordonnées à tous les niveaux.

Le quotidien civil est caractérisé par une exploitation normale des infrastructures TIC. Dans une telle situation, l'administration fédérale, la société ainsi que l'économie et les exploitants d'infrastructures critiques subissent en permanence des attaques qui doivent être reconnues ou détectées, puis repoussées par des contre-mesures. Les mesures préventives sont en première ligne prises au niveau de l'infrastructure et de l'exploitation et provoquent régulièrement des réactions sans conséquences significatives.

Une crise se manifeste par une attaque réussie ou une perturbation durable aux conséquences graves pouvant même avoir des effets sur le pays tout entier. Selon son intensité, une crise augmente le rythme de conduite au sein des structures existantes destinées à gérer la continuité et les crises. En pareille situation, il s'agit prioritairement de faire interagir des actions qui, selon les circonstances, doivent être accompagnées, au niveau national, de mesures techniques décidées par le monde politique. Dans un tel cas, la maîtrise de la crise passe en partie par la recherche de ses origines. Les exploitants des infrastructures critiques, ainsi que les fournisseurs de prestations TIC et fournisseurs de systèmes concernés, sont, sur la base de conventions, parties prenantes dans le processus décisionnel.

Objectifs de rendement et planification
Les analyses individuelles et sectorielles des risques doivent servir de base aux accords sectoriels et à la planification de la continuité. Elles doivent être étroitement élaborées ou coordonnées avec les opérateurs et les autorités compétentes. En cas de crise, les planifications doivent être établies en accord avec les autorités et les représentants de l'économie et des accords spécifiques convenus lorsque cela s'avère nécessaire. Ce processus se déroule en collaboration et en accord avec les responsables de la gestion des risques de la Confédération et ceux de l'application de la stratégie nationale pour la protection des infrastructures critiques.

La Suisse doit être en mesure, seule ou en coopération avec des partenaires étrangers, d'identifier toute attaque portée contre elle ou potentielle, de se défendre activement et, dès lors, de soutenir la gestion réactive de crise. Les organes responsables sont habilités à diriger des opérations ciblées en vue d'acquérir des informations à propos d'infrastructures d'attaque. Cela doit être prévu dans les bases juridiques correspondantes (p. ex. LSRe) et soumis aux décideurs politiques.

Mesures

Mesure 12
Les acteurs de l'économie, de la société et des autorités doivent, dans le cadre d'une étroite collaboration, renforcer et améliorer la capacité de résistance (résilience) contre les

perturbations et les incidents par une gestion appropriée de la continuité. **(DFE, DFF, DDPS, DETEC)**

Application
Le DFE, dans le cadre de la révision de la LAP, adapte ses compétences pour pouvoir analyser, en fonction des besoins, les risques et les vulnérabilités avec tous les secteurs partiels de l'approvisionnement économique du pays (AEP), en impliquant, selon la situation, les autorités compétentes (avant tout celles du DETEC et du DFF). Les résultats doivent être reportés dans les plans correspondants de gestion de la continuité et des crises. Si certains exploitants d'infrastructures critiques ne sont pas recensés par l'AEP, ils doivent être abordés par les autorités compétentes qui adapteront, au besoin, la législation dans leurs secteurs spécifiques.

MELANI soutient et intensifie l'échange volontaire d'informations entre les opérateurs d'infrastructures critiques, les fournisseurs de prestations TIC et les fournisseurs de systèmes afin de soutenir la continuité et la capacité de résistance en se fondant sur le principe de l'auto-assistance. En raison du besoin accru en capacités forensiques, du flux croissant d'informations et de l'intensification de l'échange d'informations avec les opérateurs d'infrastructures critiques et le monde économique, MELANI renforce son personnel d'ici à fin 2017. Des capacités supplémentaires sont créées dans le cadre d'une collaboration systématique avec les fournisseurs de prestations TIC et les fournisseurs de systèmes concernés.

Mesure 13
Lors d'une crise, les activités doivent avant tout être coordonnées par MELANI avec les acteurs directement concernés. Quant aux processus décisionnels des structures existantes destinées à gérer la continuité et les crises, ils sont appuyés par l'expertise requise afin de garantir une approche cohérente de la gestion de crise. Dans ce cadre, les principes de légalité de la procédure pénale doivent aussi être pris en compte. L'échange d'informations – tant au niveau national qu'international – joue un rôle important dans la gestion des crises et doit donc être assuré et coordonné. **(DFE, DFF, DDPS, DFJP)**

Application
Afin de soutenir les acteurs concernés lors d'une crise, MELANI soutient et intensifie l'échange volontaire d'informations avec les opérateurs d'infrastructures critiques et ses partenaires internationaux et garantit l'implication des services de police. Cela accroît le besoin en capacités forensiques, augmente le flux d'informations et intensifie l'échange d'informations avec les opérateurs d'infrastructures critiques et le monde économique. Des capacités supplémentaires sont créées dans le cadre d'une collaboration systématique avec les fournisseurs de prestations TIC et les fournisseurs de systèmes concernés.

Mesure 14
En cas de menace spécifique, des mesures actives d'identification des délinquants et criminels ainsi que de leurs intentions, d'investigation de leurs capacités et de dégradation de leur infrastructure doivent être prévues. **(DDPS, DFJP)**

Application
Le Service de renseignement de la Confédération devra assumer les aspects cybernétiques de son mandat pour maîtriser et assurer le suivi des cas intéressant la protection de l'Etat en

lien avec les moyens TIC. Ce processus implique la BAC comme fournisseur technique de prestations pour le SRC et le RM comme interface avec les services partenaires militaires, les alliances militaires internationales et leurs agences. Cela doit être prévu dans les bases juridiques correspondantes (principalement dans la LSRe) et soumis aux décideurs politiques.

Les résultats enregistrés par MELANI dans l'analyse de la menace et les possibilités d'investigation et de transfert des délinquants et criminels découlant du mandat légal de la poursuite pénale influent sur les mesures à prendre.

Mesure 15
Il faut veiller à ce que les procédures et processus de conduite au sein des structures existantes, qui servent à augmenter le rythme de conduite en vue de résoudre à temps les problèmes liés à une crise, tiennent compte des aspects cybernétiques. Ce processus se déroule avec l'accord des responsables de la stratégie nationale pour la protection des infrastructures critiques et des départements. **(ChF)**

Application
Lorsque la ChF est chargée par le Conseil fédéral de lui soumettre des propositions concernant les points « Détection précoce des crises » et « Gestion des crises » dans le cadre de la réforme gouvernementale, elle doit impliquer dans la procédure les partenaires compétents en matière de cyberrisques.

4.3.7 Champ d'action 7 : bases juridiques

Identification, analyse et évaluation
Une multitude de lois fédérales et d'ordonnances contiennent actuellement des bases juridiques concernant le cyberespace. La situation est cependant compliquée, car ces réglementations sont mal coordonnées et présentent, pour certaines, encore des lacunes.

Dans le cadre de l'application des mesures, les possibilités pour l'administration d'édicter, au travers de ses organes, des restrictions obligatoires en lien avec la réduction des cyberrisques doivent, au besoin, être clarifiées.

Objectifs de rendement et planification
Les bases juridiques existantes reflètent l'impact de la cybernétique sur les tâches et les responsabilités. Par conséquent, il serait inopportun d'opter pour une loi unique, en vigueur à l'échelle nationale, dédiée spécialement au cyberespace. La législation existante doit donc être adaptée en permanence aux développements de tout domaine d'application dans le cyberespace et faire l'objet de révisions. Il s'agit toutefois de déterminer impérativement en quoi consistent ces travaux et d'assurer leur cohérence.
La question de savoir dans quelle mesure il existe déjà des bases juridiques en mains des autorités permettant d'engager les acteurs concernés (en particulier les cantons, les exploitants d'infrastructures critiques et les milieux économiques) ou quelles démarches juridiques doivent être entreprises pour créer de tels pouvoirs décisionnels en cas de besoin reste encore à clarifier.

Mesures

Mesure 16
En ce qui concerne les bases juridiques existantes, il s'agit de vérifier la cohérence des mesures qu'elles imposent et leur absence de lacunes. Pour ce faire, un ordre de priorité doit être fixé pour adapter sans délai les bases qui ne seront pas mises à jour dans le cadre d'une révision périodique*.* **(DFF)**

Application
L'organe de coordination et de concrétisation de la stratégie élabore pour fin 2013, en collaboration avec les départements, un premier aperçu, tenant compte des mesures présentées, de la nécessité urgente de légiférer et de procéder à des révisions dans le domaine de la cybernétique. Pour ce faire, il faut aussi veiller à ce que l'échange d'informations avec des tiers et le traitement des données soient, de par la loi, aussi normalisés que possible. En outre, d'éventuelles obligations plus étendues doivent être communiquées aux cantons, aux exploitants d'infrastructures critiques et aux milieux économiques. La constitutionnalité des réglementations proposées doit être assurée, en collaboration avec l'OFJ. Les lacunes identifiées comme prioritaires dans la législation et les adaptations légales nécessaires doivent être abordées par les départements compétents dans le cadre d'un avant-projet prêt à faire l'objet d'une procédure de consultation et accompagné d'un rapport explicatif, tous deux devant être élaborés d'ici fin 2014.

4.3.8 Organe de coordination et de concrétisation de la stratégie

L'élaboration et l'application des mesures relèvent des organes responsables concernés dans le cadre de leur mission et se déroulent *en collaboration* avec leurs partenaires des autorités compétentes (à l'échelon de la Confédération, des cantons et des communes), des milieux économiques (opérateurs et associations) et de la société. Les organes compétents garantissent l'implication de ces acteurs.

Un organe de coordination et de concrétisation de la stratégie, dépendant du Département fédéral des finances (DFF), appuie, en étroite collaboration avec les organes responsables, l'application et l'exécution permanentes des mesures exigées*.* Ce processus doit s'accomplir sur une période de quatre à six ans. L'organe de coordination doit collaborer étroitement avec les organes de coordination et autres bureaux existants dans le cadre d'autres stratégies de la Confédération et éviter les doublons.

La fin de la phase de concrétisation – soit après l'entrée des processus et adaptations en question dans un cycle régulier d'exploitation – marque celle de l'organe de coordination et de concrétisation de la stratégie. La Centrale d'enregistrement et d'analyse pour la sûreté de l'information reprend, si nécessaire, le rôle de coordonnateur et de gestionnaire suite aux procédures de concrétisation.

Les tâches de l'organe de coordination et de concrétisation de la stratégie sont les suivantes :

- diriger un comité interdépartemental de pilotage chargé de coordonner les étapes de concrétisation à l'échelon de la Confédération ; celui-ci se compose de représentants des offices fédéraux compétents ; les départements désignent eux-mêmes leurs représentants ;

- encadrer, en collaboration avec le mécanisme de consultation et de coordination du réseau national de sécurité (MCC RNS), un groupe spécialisé « Cyber » composé de représentants de la Confédération, des cantons et des communes ainsi que des représentants des exploitants d'infrastructures critiques, de l'économie et de la société ; ce groupe favorise l'harmonisation de l'information entre les partenaires ainsi que l'amorçage et la coordination de solutions communes aux problèmes ;
- élaborer un plan de mise en œuvre détaillé avec les organes responsables à l'échelon de la Confédération ; ce plan comprend la concrétisation pour les domaines concernés et les adaptations des ressources et des bases juridiques ;
- informer une fois par an le Conseil fédéral de l'état de la procédure de concrétisation ;
- veiller à la coordination de la procédure utilisée par les départements compétents dans l'application des mesures, pour autant que celles-ci concernent la législation, en particulier pour les projets de révision futurs ou en cours (FOGIS, LPol, LSRe, LAP, LSCPT) ;
- surveiller la concrétisation de la stratégie nationale de protection de la Suisse contre les cyberrisques en tenant compte de la politique de gestion des risques menée par la Confédération, de la stratégie nationale pour la protection des infrastructures critiques et de l'analyse nationale des dangers « Risques suisses » (DDPS-OFPP) ainsi que de la stratégie du Conseil fédéral pour une société de l'information en Suisse (DETEC-OFCOM) ;
- examiner avec les organes responsables une simplification et un allègement des moyens et systèmes d'annonce ;
- étudier avec les organes responsables des synergies possibles (p. ex. dans le domaine technico-opératif) ;
- coordonner et appliquer les mesures 7, 8 et 15 avec les offices et acteurs compétents et apporter, au besoin, son appui en fournissant des données techniques lors de l'application de la mesure 1 ;
- vérifier après cinq ans, la stratégie nationale de protection de la Suisse contre les cyberrisques et sa concrétisation en relation avec le développement du domaine de la cybernétique et des mesures prises ; établir un benchmarking systématique s'y rapportant.