16 avril 2015

Concept de gestion nationale des crises à caractère cybernétique (mesure 15 SNPC)

1. Contexte

La Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) prévoit diverses mesures pour le champ d'action Gestion de la continuité et des crises, notamment la mesure 15, qui s'intéresse plus particulièrement au rythme de conduite :

« Elaboration d'un concept pour des procédures et processus de conduite permettant une résolution des problèmes en temps opportun : *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 ».*

Afin de concrétiser cette mesure, la Chancellerie fédérale a élaboré un concept (pour le niveau fédéral), qui a été approuvé le 11 février 2014 par le comité de pilotage de la SNPC.

Aussi le présent document complète la mesure 15 en y intégrant les cantons et vise à décrire les processus et interfaces entre Confédération et cantons. Etabli par la Chancellerie fédérale et le secrétariat du Réseau national de sécurité, il a été soumis à divers services de la Confédération et des cantons ainsi qu'à divers exploitants d'infrastructures critiques. Il s'agit uniquement d'un document de travail pour les séquences de formation en gestion des crises au niveau étatique lorsque le scénario comprend l'aspect des cyberrisques.

2. Crises à caractère cybernétique

Une cyberattaque, une erreur système ou la négligence d'un collaborateur peuvent causer une atteinte à l'intégrité ou à la confidentialité des informations, ou encore réduire la disponibilité d'un système informatique. Le réseau internet peut être utilisé comme vecteur ou devenir lui-même une cible. Les possibilités vont d'une attaque par déni de service opérée par des activistes ou des maîtres-chanteurs à une manipulation de processus bancaires par des criminels, en passant par l'espionnage et les cyberattaques effectués par des Etats ou des acteurs non étatiques – on peut penser à des actes de sabotage visant les infrastructures critiques ou l'intégrité du système financier dans le but de déstabiliser le fonctionnement du pays. Si de telles actes conduisent à une situation grave, à elles seules ou en combinaison avec d'autres éléments, et que l'aspect de la cybersécurité reste un élément essentiel du problème à régler pour la Confédération et les cantons, on peut alors parler d'une crise nationale à caractère cybernétique. La situation normale peut devenir une situation particulière voire une situation extraordinaire[1]. Chaque crise est marquée au début par une phase d'incertitude concernant la nature du danger ou de la menace ainsi que son étendue et ses répercussions. Une seule menace crédible dirigée contre la cybersécurité peut conduire à une situation de crise majeure.

Evaluer la situation dans un contexte de cyberrisques, afin de savoir si elle est due à un problème technique, si elle comporte des implications politiques et évaluer sa dimension, représentent un premier défi à relever. Les responsables sont aussi soumis à la pression du temps dans leur recherche de décisions appropriées.

[1] Pour les définitions, voir les instructions du 24 octobre 2007 sur les mesures organisationnelles à prendre dans l'administration fédérale pour maîtriser les situations particulières ou extraordinaires, p. 1

Un scénario de crise de nature sécuritaire peut également comporter un aspect de cyberrisque par le simple fait qu'un abus du cyberespace pourrait aggraver considérablement la situation, faisant du rétablissement de la cybersécurité une priorité de la gestion de la crise.

3. Conduite coordonnée et réseau spécialisé

La gestion des crises et des situations d'urgence, contrairement à celle des risques, repose non pas sur des scénarios, mais des processus. En effet, tant l'organisation de la conduite que les processus de décision doivent être constants, indépendamment de la nature de la crise. Cet élément revêt une importance toute particulière lorsque la crise affecte la réputation, la liberté d'action ou l'existence même d'une organisation : celle-ci doit pouvoir compter sur les mêmes processus et sur les décisions des mêmes hauts responsables qu'à l'accoutumée. Ce principe vaut aussi bien pour la Confédération (Conseil fédéral), que les gouvernements respectifs des canton. La gestion générale de la crise (procédures et processus de conduite) ne dépend donc pas d'un scénario en particulier. Toutefois, les structures et organes de conduite de la Confédération et des cantons constituent en cas de crise nationale un réseau structuré en fonction de la crise et requérant une coordination étroite des processus de décision respectifs.

Les organes de la Confédération, des cantons ou de tiers (infrastructures critiques) affectés à la veille et au traitement d'un risque spécifique varient, quant à eux, en fonction du scénario. Ils constituent un réseau spécialisé. Lorsqu'un risque en particulier prend de l'importance et pourrait déboucher sur une crise majeure, ils leur appartient de mettre en place la gestion opérationnelle. Ils procèdent à une première appréhension du problème, fournissent une évaluation de la situation et assument la tâche de conseiller technique auprès des organes de décision. Ils contribuent ensuite à la concrétisation des mesures décidées sur le plan stratégique. A la Confédération et pour le domaine des cyberrisques, cet organe spécifique de surveillance est la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI). Dans les cantons, ce rôle est confié aux responsables de l'informatique et de la sécurité de l'information, organisés – pour certains – sous forme d'équipes spécialisées.

4. Gestion coordonnée

4.1 Coopération cantons – Confédération

Faire face à une crise dans une société fortement interconnectée requiert d'une part une coordination étroite des organes de crise et des décideurs à tous les échelons, et d'autre part la mise en commun du savoir spécifique détenu tant par l'Etat que par les acteurs privés. Les responsabilités tant au niveau de la Confédération que des cantons sont clairement fixées. La gestion générale des crises (procédures et processus de conduite), y compris celles comportant des éléments cybernétiques doit rempli les trois objectifs suivants :

1. Fournir une description de la situation actuelle, homogène et complète
2. Créer les condition cadres favorables qui permettent aux gouvernements (fédéral et cantonal de prendre des décisions
3. Etablir une stratégie de communication et définir les mesures qui en découlent.

En cas de crise à caractère cybernétique, il faut recourir au savoir et aux capacités spécifiques de services de l'Etat et de l'économie privée, et les organiser de manière à pouvoir les intégrer rapidement au processus de conduite. Pour cela, il faut tirer profit des partenariats public-privé déjà établis, et échanger des informations dans toute la mesure permise par le droit. Comme dans d'autre type de crise, l'armée pourra apporter son aide aux autorités civiles dans le respect du principe de la subsidiarité.

Les points suivants requièrent une coordination entre cantons et Confédération :

- Evaluation et présentation communes de la situation

- harmonisation des options stratégiques et synchronisation des décisions
- gestion des ressources
- gestion de la continuité coordonnée
- élaboration et communication communes d'informations.

4.2 Implication des infrastructures critiques

La gestion des crises au niveau national doit relever un défi en particulier, soit l'intégration des infrastructures critiques. Celles-ci peuvent en effet jouer un rôle essentiel tant à l'origine d'une crise (elles constituent des objectifs stratégiques) que dans ses conséquences (alimentation de base de l'économie et de l'Etat). Elles peuvent donc elles-mêmes être la cible d'une attaque, portant par exemple sur un réseau numérique, (Swisscom) ou un réseau électrique (Swissgrid). Par conséquent :

- Il faut s'assurer que ces infrastructures disposent d'une organisation de crise, connue, avec des interfaces définies vers la Confédération et les cantons tant sur les plans opérationnel, politique et stratégique.
- Les infrastructures critiques fournissant des prestations à l'échelon national et elles ne peuvent pas se limiter à une interface cantonale. Leur interruption peut avoir des répercussions sur le plan national voire international. Il faut donc une interface directe vers la Confédération sur tous les plans (opérationnel, politique et stratégique).
- La coordination des infrastructures critiques requiert la collaboration étroite de la Confédération et des cantons, sous la responsabilité de la Confédération.

5. Séquences communes de formation

5.1. Séminaire stratégique du 11 juin 2015

Les modules de formation servent à préciser quelles interfaces et quels processus interviennent lors d'une cybercrise d'ampleur nationale. L'objectif est d'améliorer les structures et la coordination.

La cyber-landsgemeinde de 2013 a proposé un premier module d'entraînement sous forme de séminaire stratégique réunissant des représentants de la Confédération, des cantons et des exploitants d'infrastructures critiques. Ce séminaire aura lieu le 11 juin 2015. Son but est de montrer les structures et processus de la gestion des crises à caractère cybernétique au niveau cantonal ainsi que les interfaces avec le niveau fédéral.

5.2. Autres exercices cantonaux et nationaux

D'autres séquences de formation sont envisageables, sous une forme qui reste à définir. Par exemple, il serait possible de simuler les fonctions clé de la gestion des crises pour la Confédération, les cantons et les tiers dans le cadre d'un module d'entraînement, afin de préciser encore mieux les besoins en matière de coordination et prévenir ainsi les risques de frictions.

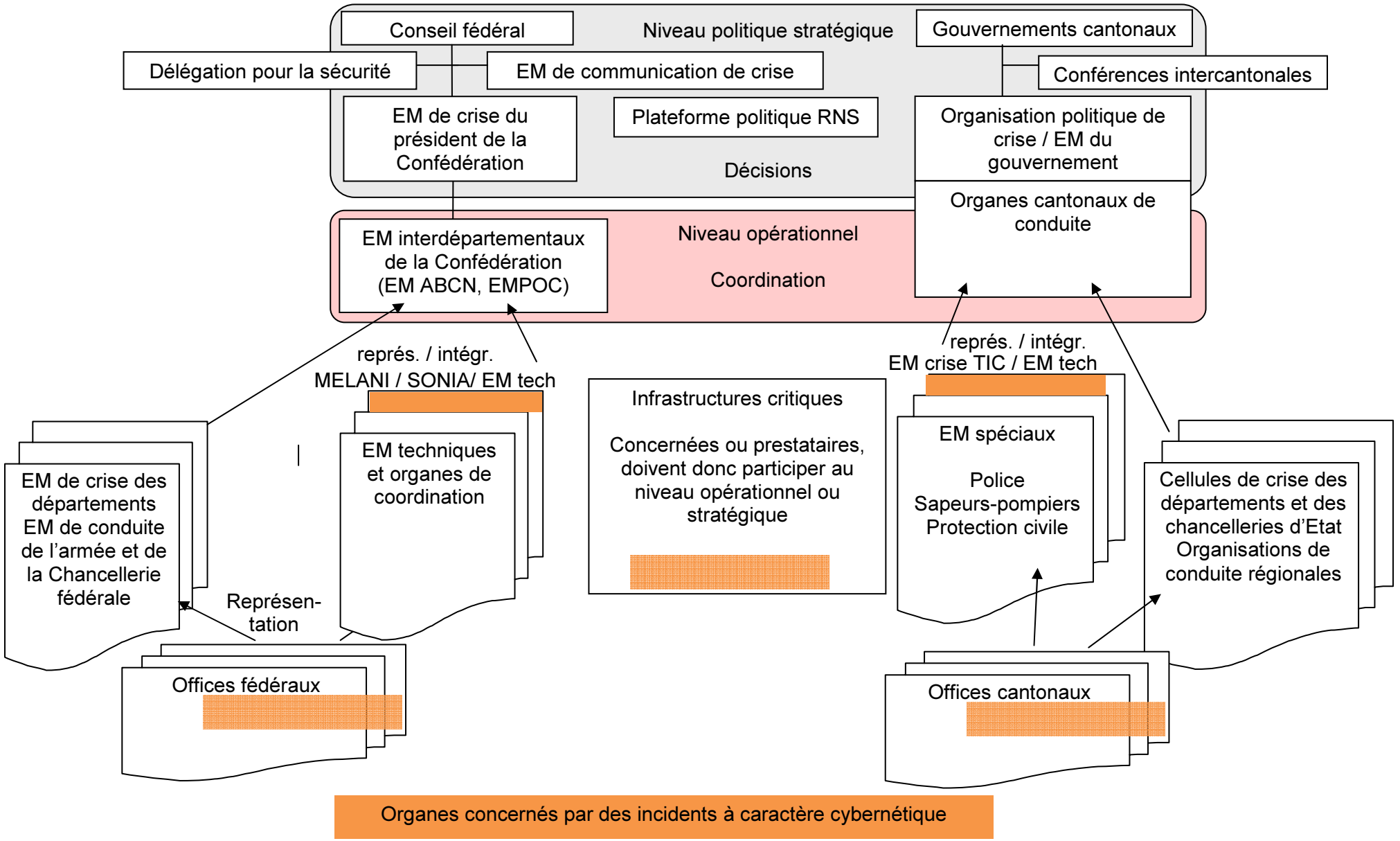
On peut aussi imaginer des exercices de prise de décision thématiques, organisés par les cantons pour leurs organes de conduite.

Il serait également souhaitable de s'entraîner au plus haut niveau, en organisant par exemple un exercice d'état-major global intégrant la Confédération, les cantons et les infrastructures critiques.

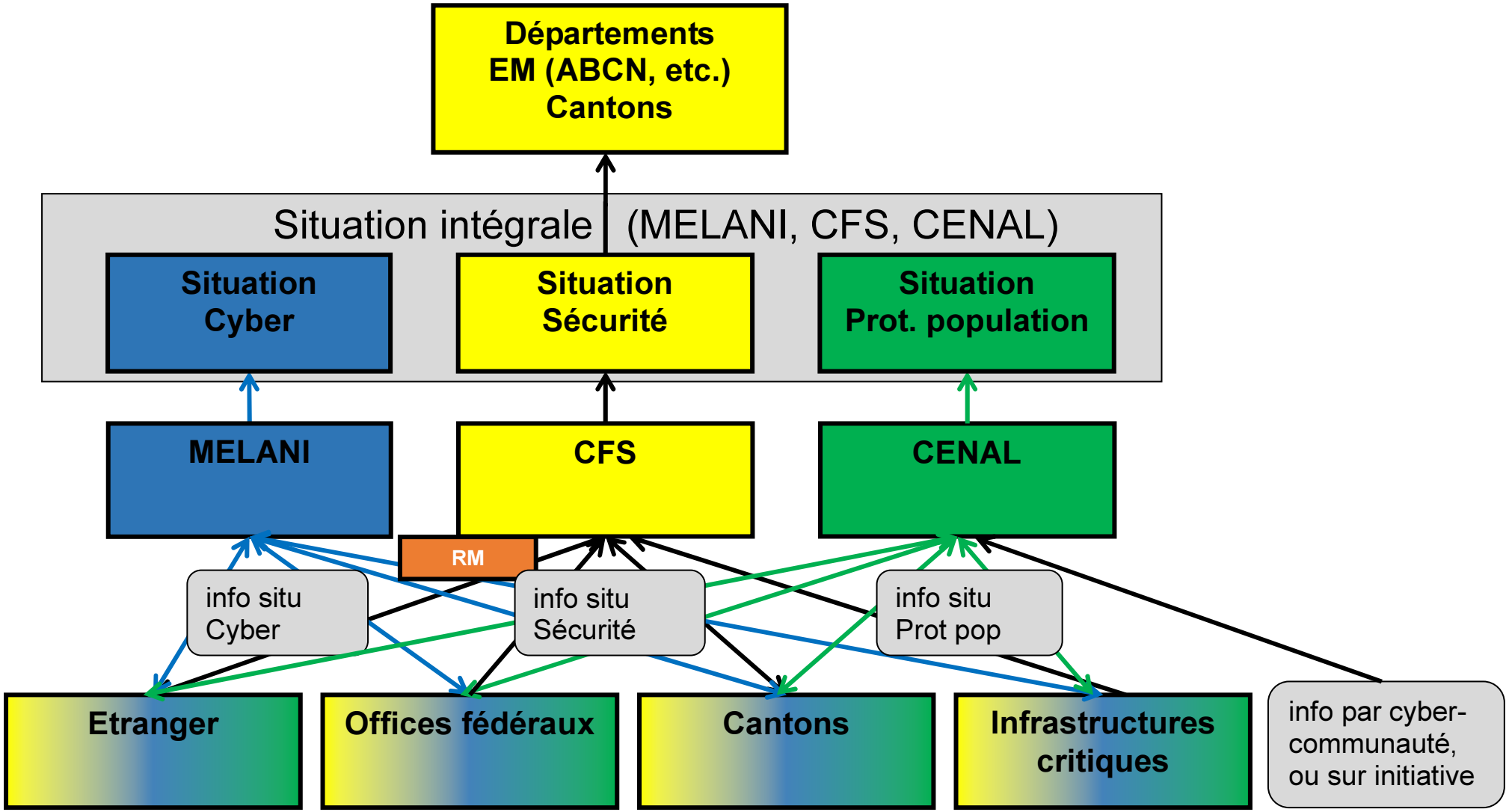
Annexe 1 Aspects principaux d'une crise à caractère cybernétique

Risque élevé d'aggravation de la situation
– Cybersécurité touchée, avec risque élevé que la situation s'aggrave – Conséquences graves déjà du fait de l'interruption inopinée des services informatiques – Paralysie de la vie quotidienne et de l'activité économique – Dommages aux infrastructures – Pression élevée pour le rétablissement des réseaux numériques
Dimension technique
– Défi informatique initial pour le rétablissement de la continuité opérationnelle – Première étape touchant les spécialistes des questions informatiques et techniques – Incident initial dans le cadre d'une situation ordinaire – Aggravation de la situation requérant une gestion de la crise (communication, questions juridiques, réparation de dommages consécutifs, etc.)
Sécurité de l'information (intégrité des données et des informations)
– Brèche dans l'intégrité, la confidentialité ou la disponibilité de données dont l'Etat est garant (autorités, infrastructures critiques) – Données détournées, manipulées ou utilisées à des fins non autorisées (faux certificats d'autorités, utilisation de données personnelles de citoyens) – Première phase touchant les unités administratives concernées par la sécurité de l'information puis, en cas d'aggravation, les organes de décision politiques
Baisse de la confiance placée dans les moyens informatiques et les exploitants de systèmes
– Baisse de la confiance placée dans l'Etat et les exploitants de systèmes informatiques si les problèmes de sécurité ne sont pas réglés et les attaquants identifiés et neutralisés – Indignation générale au vu de l'absence de protection des données personnelles – Répercussions sur certains systèmes, sur certains exploitants de systèmes, sur les échanges de courriels avec les services étatiques, désormais évités – Dommages économiques considérables et entrave au fonctionnement de l'administration
Pression considérable sur les organes de décision
– Caractère essentiel d'une infrastructure informatique pour tous les aspects de la vie, y compris pour la gestion des crises par la Confédération, les cantons et les infrastructures critiques – Conséquences politiques d'une panne d'importance dans les systèmes de l'administration – Forte pression exercée par l'opinion publique et les médias sur les organes politiques responsables, en fonction de l'étendue des dommages et du caractère sensible des informations – Exigences visant à rétablir la sécurité des informations, juguler la perte de données, réparer ou contenir les dommages de manière compétente, neutraliser et poursuivre pénalement les auteurs
Eléments dynamiques de la menace
– Augmentation des abus potentiels du cyberespace (possibilités, disposition) – Evolution des cibles et des méthodes (cheval de Troie, porte dérobée, manipulation de système de commandes d'installations industrielles, surveillance des communications, etc.) – Intrusion dans des réseaux informatiques, conversion de téléphones mobiles en stations d'écoute, recherches licites ou illicites par le biais d'Internet – Destruction définitive ou modification insidieuse de données par des maliciels – Réactions en chaîne fatales déclenchées par des attaques visant les infrastructures critiques (par la manipulation de systèmes de commandes portant sur l'approvisionnement énergétique, la communication et les transports, ou par l'intrusion dans les systèmes financiers) – Discrédit jeté sur certaines personnes, les autorités, l'Etat, par le vol de données sensibles – Influence sur les processus et décisions politiques – Perturbation de la stabilité et du développement économiques – Accès possible à des informations par une attaque provenant de l'étranger (intégration internationale des réseaux informatiques) – Espionnage des rivaux politiques ou économiques déjà possible même pour de petites organisations – Attaques informatisées appuyées par l'intervention d'agents au sens traditionnel

Annexe 2 ***Structures de conduite cantons – Confédération et implication des infrastructures critiques***



Annexe 3 *Structure permettant un relevé de la situation lors d'une crise à caractère cybernétique*



Compléments d'explication pour le schéma de l'annexe 2

Conseil fédéral	• désigne le département responsable ou confie au président la gestion de la crise • prend les décisions
EM interdepartementaux de la Confédération	• est dirigé par un membre du Conseil fédéral • inclut le secrétaire général du département responsable • crée les bases de décision du Conseil fédéral après procédure de co-rapport simplifiée • définit la stratégie et les mesures de communication
Plateforme politique du Réseau national de sécurité (RNS)	• participe à la définition d'une stratégie commune entre cantons et Confédération • coordonne les décisions des gouvernements (cantons et Confédération) • définit les priorités en matière d'approvisionnement, de transports et de ressources • propose des messages communs pour la communication de crise
EM de coordination interdépartemental de la Confédération EM ABCN – EMPOC	• fournit aux organes de gestion de la crise une vue d'ensemble de la situation sur le plan stratégique • prépare des bases de décision pour le Conseil fédéral (consultation des offices) • constitue l'état-major du département responsable • inclut des représentants de haut rang des départements concernés
Gouvernements cantonaux	• désignent la direction responsable et attribuent au directeur la tâche de gérer la crise • prennent les décisions
EM des gouvernements cantonaux	• sont facultatifs (certains gouvernements cantonaux traitent directement avec l'organe cantonal de conduite) • sont dirigés par un conseiller d'Etat • incluent les secrétaires généraux des autres directions • traitent la dimension politico-stratégique de la crise et élaborent des options • définissent la stratégie et les mesures de communication
Organes cantonaux de conduite	• fournissent une vue d'ensemble de la situation sur le plan stratégique (cf. annexe 2) • préparent des bases de décision pour le gouvernement cantonal • définissent la stratégie et les mesures de communication
EM spécialisés (SONIA) EM cantonaux spécialisés Organes de coordination (SSC, CTE, Météosuisse, télématique, protection ABC, LAINAT)	• coordonnent sur le plan opérationnel les bases de décision des gouvernements ou les mesures de concrétisation (consultation des offices) • prennent les décisions dans leur sphère de compétence et ordonnent les mesures opérationnelles • exécutent les décisions des gouvernements sur le plan opérationnel