Sécurité des infrastructures de radiodiffusion et de télécommunication en Suisse lors de situations extraordinaires

Rapport du Conseil fédéral aux commissions de la politique de sécurité des Chambres fédérales

du 30 novembre 2001

Table des matières

1 INTRODUCTION 3

1.1 Mandat 3

1.2 Limitations 3

1.3 Procédure 4

1.4 Définitions 4

2 PRINCIPES 5

2.1 Dépendances et dangers de la société de l'information 5

2.2 Mandat de politique de sécurité 6

2.3 Bases légales 6

3 EXIGENCES DE SÉCURITÉ 7

3.1 Généralités 7

3.2 Détails 8

4 RISQUES ET MESURES 11

4.1 Méthode utilisée pour l'analyse des risques 11

4.2 Analyse des risques et mesures nécessaires 12
4.2.1 Dangers liés à la technique 13
4.2.1.1 Surcharge du réseau *(1)* 13
4.2.1.2 Points critiques et réseaux intelligents centralisés *(2)* 13
4.2.1.3 Développement technologique *(3)* 14
4.2.1.4 Technologies étrangères *(4)* 14
4.2.1.5 Centres d'exploitation de réseaux à l'étranger *(5)* 14
4.2.1.6 Technologie par satellite *(6)* 15
4.2.1.7 Monoculture technique *(18)* 15
4.2.1.8 Problèmes de réception *(7)* 15
4.2.2 Branche informatique 16
4.2.2.1 Privatisation *(8)* 16
4.2.2.2 Fragmentation des entreprises *(9)* 16
4.2.2.3 Internationalisation *(10)* 17
4.2.3 Personnel *(11)* 17
4.2.4 Influences extérieures 18
4.2.4.1 Sabotage *(12)* 18
4.2.4.2 Panne d'énergie *(13)* 18
4.2.4.3 Catastrophes anthropiques *(14)* 19
4.2.4.4 Catastrophes naturelles *(15)* 19
4.2.5 Organisation 19
4.2.5.1 Manque de compatibilité (16) 19
4.2.5.2 Problème dans le domaine VRK-OUC 77 (VRK-UKW 77) *(17)* 19

4.3 Aperçu des risques et des mesures 21

5 SYNTHESE DES RESULTATS 23

Annexes

Annexe 1 : Membres du groupe de travail

Annexe 2 : Structure

1 Introduction

1.1 Mandat

Dans le cadre de la discussion politique concernant les projets de Swisscom de vendre ses activités de radiodiffusion, il s'est posé la question suivante : dans quelle mesure la Confédération, en tant qu'actionnaire principale, doit-elle conserver un pouvoir de disposition sur les infrastructures essentielles d'information et de communication, afin de garantir les intérêts nationaux en matière de sécurité ? Par ailleurs, différentes interventions parlementaires demandent des mesures visant à garantir ces exigences de sécurité. Dans ses réponses, le Conseil fédéral a annoncé que les besoins en question seraient analysés dans le cadre d'un groupe de travail interdépartemental, chargé d'examiner par quels moyens il fallait garantir que ces besoins soient gérés. Un groupe de travail s'est donc attelé à la tâche sous la direction du DETEC (OFCOM). Ce rapport en présente les résultats.

Le groupe de travail a très vite constaté que les intérêts nationaux concernant la sécurité des infrastructures électroniques de communication devaient être considérés dans leur globalité, et non pas seulement sous l'angle de l'accès à ces infrastructures par le biais d'installations appartenant à la société qui les exploite. Il faut donc aborder dans leur globalité les risques qui menacent ces infrastructures. Sur cette base, des mesures doivent être définies qui contribuent à éliminer ou du moins à limiter les risques en question.[1]

Le présent rapport n'est qu'un instantané de la situation actuelle; l'analyse des risques et l'élaboration de mesures conséquentes doivent être effectués constamment par les organes concernés.

1.2 Limitations

Les situations de crise dans le domaine de la société de l'information peuvent concerner aussi bien les pouvoirs publics que l'économie privée. Tous les acteurs de la société de l'information sont eux-mêmes responsables, en dernier lieu, de la sécurité de leurs infrastructures informatiques et de communication.[2] Toutefois, étant donné qu'il s'agit d'infrastructures qui sont largement mises en réseau, il faut pour pouvoir garder une vue d'ensemble du système que cette supervision soit coordonnée par l'État, l'économie et le monde scientifique. Dans ce contexte, différents organes étatiques, semi-étatiques ou privés ont déjà été créés ou sont en voie de l'être, chargés de la sécurité de l'information *au sens large*. Il s'agit pour l'essentiel de la fondation privée InfoSurance[3], de l'office de milice ICT-I[4], de l'état-major "Sécurité de l'information"[5]. Dans le domaine militaire, c'est le groupe de projet "Information Operations", au sein du DDPS, qui est chargé de la guerre de l'information et des autres sujets connexes. En outre, au niveau de la Confédération, il est prévu de créer un "Organe de coordination Information Assurance"[6]. En juin 2001, la Formation à la conduite stratégique a organisé un exercice INFORMO, à l'occasion duquel ces organes, et en premier lieu l'état-major "Sécurité de l'information", ont pu tester leur positionnement et leur fonctionnement.

[1] Il faut préciser que dans certains domaines, des mesures ont déjà été prises (concrétisées ou non, selon le contexte). Cette différence est importante, notamment pour l'analyse des risques (chiffre 4), domaine dans lequel il est essentiel que les mesures déjà concrétisées soient prises en compte en tant que telles.

[2] Rapport du Conseil fédéral à l'Assemblée fédérale sur la politique de sécurité de la Suisse (RAPOLSEC B 2000), p. 65.

[3] www.infosurance.ch

[4] Sur le plan de l'organisation, rattaché à l'Office fédéral de l'approvisionnement économique du pays, domaine Infrastructure d'information et de communication.

[5] Sur le plan de l'organisation, rattaché à l'Unité de stratégie informatique de la Confédération.

[6] Voir à ce propose le concept 'Information Assurance' du 17 mai 2000 du Groupe de coordination Société de l'information.

Les résultats, qui sont en cours d'évaluation, seront soumis au Conseil fédéral dans le courant de cet automne.

Dans le cadre de la problématique posée dans ce rapport, il s'agit en revanche des besoins de sécurité des pouvoirs publics en cas de situations extraordinaires *au sens étroit*, par conséquent de leurs besoins lorsqu'il s'agit de gérer une crise. Les intérêts des privés ayant une signification nationale sont pris en compte principalement dans le cadre de l'approvisionnement économique du pays. Les cas recensés ici sont avant tout des incidents et des perturbations qui, du fait de leur étendue et de leur intensité, pourraient déboucher sur des pénuries graves que l'économie ne maîtriserait pas seule. En général, il s'agit d'événements qui touchent plusieurs secteurs, et qui doivent par conséquent être traités en coordination par plusieurs secteurs.

S'agissant de la sécurité dans le domaine de l'information et de la communication, on fait en général une distinction entre les aspects relatifs à l'infrastructure et les aspects relatifs au contenu. La responsabilité des contenus (p.ex. cryptage d'un bout à l'autre d'une communication) est d'une façon générale attribuée directement à l'utilisateur final ou aux producteurs de contenu (p.ex. parties de programmes radiodiffusés), alors que la sécurité concernant l'infrastructure doit être garantie en principe par l'opérateur de l'infrastructure technique de communication (mise en place et exploitation).

1.3 Procédure

Dans un premier temps, l'OFCOM a recensé au sein de l'administration fédérale et parmi les cantons les entités qui avaient des besoins en matière de sécurité, et a fourni des informations sur le mandat et la procédure prévue.[7] A cette occasion, les organes contactés ont été invités à identifier d'autres demandeurs et à fournir, dans le cadre d'un questionnaire, une première série d'informations. Les responsables de la coopération cantonale en matière de sécurité ont ensuite été intégrés à l'équipe chargée de la coopération nationale déjà représentée dans le groupe de travail. La structure prévue[8] devait d'une part servir d'instrument de travail aux entités interrogées, et d'autre part faciliter le travail de l'OFCOM lors de l'évaluation des résultats. Après un premier examen des réponses remises, qui se sont révélées très hétéroclites quant à l'étendue et au degré de concrétisation, une première séance plénière a été menée le 27 mars 2001 avec pour objectif de trouver une position commune concernant la forme des questions et la suite de la procédure, de compléter et concrétiser les résultats obtenus, et d'identifier les éventuels terrains communs. Ces premières conclusions, une fois mises en forme, ont été soumises au groupe de travail par le biais d'une notice d'information le 2 avril 2001. Le 16 mai 2001, un atelier d'une journée a eu lieu sur le thème de l'analyse des risques, auquel ont participé certains membres seulement du groupe de travail. En parallèle, des discussions informelles se sont déroulées entre différents membres du groupe. Par un courrier daté du 31 juillet 2001, le groupe de travail (ainsi que d'autres organes intéressés) a reçu pour consultation la version 1.0 du rapport. Les nombreux commentaires inspirés par le rapport ont permis de concrétiser ou de développer les résultats, voire de les corriger, et ont été intégrés dans la version 2.0. Une fois réglés les derniers détails de contenu, le rapport (version 2.2) a été approuvé lors de la deuxième séance plénière le 3 octobre 2001. Enfin, après quelques adaptations, la version définitive 2.3 a vu le jour.

1.4 Définitions

Pour des raisons de cohérence et pour éviter les malentendus, les définitions suivantes ont été adoptées.

[7] Les noms des membres du groupe de travail sont indiqués dans l'annexe 1. Outre les représentants des entités ayant des besoins en matière de sécurité, le groupe comprend également des représentants des fournisseurs de service universel.

[8] Voir annexe 2.

Situation extraordinaire :[9]

Situation dans laquelle les processus administratifs normaux en usage dans de nombreux domaines et secteurs ne suffisent pas à résoudre les problèmes et à relever les défis, tels que les catastrophes naturelles affectant sérieusement l'ensemble du pays ou les faits de guerre.

> Par opposition :
>
> *Situation normale :* Situation dans laquelle les processus administratifs ordinaires suffisent à gérer les problèmes et à relever les défis.
>
> *Situation particulière :* Situation dans laquelle les processus administratifs normaux ne suffisent plus à gérer certaines tâches de l'État. A la différence de la "situation extraordinaire", l'activité gouvernementale touchée n'est cependant que sectorielle. Ici, ce sont les besoins visant une concentration rapide des moyens et une simplification de la procédure qui s'imposent.

D'une manière générale, les affirmations de ce rapport sont aussi valables pour les situations particulières; celles-ci ne se différencient des situations extraordinaires que par l'étendue et l'intensité de l'événement. Il n'est donc pas fait de véritable distinction entre la situation particulière et la situation extraordinaire dans les pages suivantes.

Crise :

Synonyme à la fois de *situation particulière* et de *situation extraordinaire.*

Sécurité (concrètement) :

Disponibilité minimale (y compris intégrité) des infrastructures d'information et de communication pour donner l'alarme, informer et gérer les situations extraordinaires, afin de garantir la capacité de décision et de gestion concernant les intérêts nationaux.[10]

Infrastructure de radiodiffusion et de télécommunication (partie de l'infrastructure d'information et de communication) :

Dans le contexte du présent rapport, ce terme désigne les systèmes des réseaux de radiodiffusion et de télécommunication ainsi que les ordinateurs et autres installations techniques utilisés dans ce contexte, servant à transmettre des données, la voix ou des images et du son. Dans un sens plus large, on entend également, outre les composantes techniques, le savoir-faire nécessaire à la construction, l'exploitation et l'entretien de ces infrastructures. En revanche, les systèmes servant uniquement à enregistrer et traiter les informations ou les systèmes de production de programmes radio et télévision ne sont pas concernés.

2 PRINCIPES

2.1 Dépendances et dangers de la société de l'information

La technologie de l'information joue un rôle clé à l'heure actuelle. Disposer d'infrastructures d'information et de communication sûres est une condition indispensable non seulement pour le développement économique, mais également pour le bon fonctionnement du gouver-

[9] Basé sur le RAPOLSEC 2000, annexe "Définitions", p. 82.

[10] Dans un sens plus large, la sécurité comprend aussi des aspects liés au contenu tels que la confidentialité, l'authenticité et le caractère obligatoire des informations.

nement et de l'administration. Cette dépendance va devenir de plus en plus forte, ce qui implique davantage de risques et de dangers. Au vu de cette évolution, les concepts de sécurité et la planification d'urgence (contingency planing and disaster recovery) revêtent une importance capitale.

Lors de situations extraordinaires, les besoins en matière d'information et de communication peuvent devenir considérablement plus importants, selon la situation et le domaine. Les points essentiels ici sont l'acquisition d'informations, la conduite des opérations dans un contexte de crise et l'information à la population. L'expérience montre que les crises deviennent souvent aussi des crises de l'information. Il n'est pas rare que le problème provienne d'une infrastructure peu ou pas disponible.

Il en résulte logiquement que les systèmes d'information et de communication peuvent être très sensibles, selon le type de situation extraordinaire qui survient. En tous les cas, parallèlement à la complexité et à la dépendance croissante des systèmes, on constate une augmentation des abus et de l'exploitation volontaire des points faibles de ces systèmes, qu'il s'agisse de l'œuvre de pirates informatiques, de groupes plus ou moins grands ou même d'Etats étrangers. Les motivations peuvent être de nature très diverse: politico-idéologiques, religieuses, économiques, criminelles.

2.2 Mandat de politique de sécurité

Le Conseil fédéral a déjà reconnu l'importance des moyens d'information et de communication dans son rapport sur la politique de sécurité de la Suisse (RAPOLSEC 2000).[11] A cette occasion, il souligne l'importance d'une information au public qui soit à la fois fiable, claire et rapide. Outre les médias civils, le Conseil fédéral peut également faire appel, si la situation l'exige, à l'Etat-major du Conseil fédéral Division Presse et Radio (EM CF DIPRA). Cet état-major est en principe mis en fonction selon le principe de subsidiarité, c'est-à-dire lorsque les médias civils ne sont plus à même d'accomplir leur mission.[12]

L'objectif principal du Conseil fédéral est de garantir la capacité de décision et de gestion de la Suisse, et de créer des conditions générales permettant d'assurer le bon fonctionnement de la société de l'information en Suisse. Il est nécessaire pour cela de disposer d'une vision d'ensemble du système et d'une procédure coordonnée, en particulier pour ce qui est de l'identification des infrastructures vitales pour le pays, de la sensibilisation, de la formation d'experts, de l'évaluation constante des risques, de la capacité à repérer les dangers et à donner l'alarme, du rassemblement immédiat des décideurs, ainsi que de la construction d'infrastructures de sécurité communes. En outre, le Conseil fédéral reconnaît qu'il est impossible d'obtenir une protection totale par un investissement *raisonnable*, raison pour laquelle il convient de prendre des mesures de sécurité *adaptées* en se basant sur une analyse des risques fondée.

La problématique esquissée au chiffre 1.2 du présent rapport représente une partie essentielle de ce mandat global de politique de sécurité.

2.3 Bases légales

Dans l'état actuel de nos connaissances, les bases légales suivantes sont les principaux textes fournissant, au niveau fédéral, des principes juridiques relatifs aux infrastructures d'information et de communication lors de situations extraordinaires :

- Loi sur les télécommunications (LTC; RS 784.10), chapitre 8 : Intérêts nationaux importants (art. 47 s.)
- Ordonnance sur les services de télécommunication (OST; RS 784.101.1), chapitre 6 : Intérêts nationaux importants (art. 66 ss.)

[11] Voir chiffres 3.1.7 et 6.7 RAPOLSEC B 2000.

[12] Art. 2, al. 1, de l'ordonnance concernant l'état-major du Conseil fédéral Division Presse et Radio.

- Loi fédérale sur la radio et la télévision (LRTV; RS 784.40), art. 6 : Sécurité publique; obligation de diffuser
- Ordonnance sur l'informatique et la télécommunication dans l'administration fédérale (RS 172.010.58)
- Loi fédérale sur l'approvisionnement économique du pays (LAP; RS 531; princip. art. 2 et 22 ss.)
- Ordonnance sur l'organisation et les tâches de l'approvisionnement du pays (RS 531.11)
- Ordonnance sur la coordination des transmissions dans le domaine de la défense générale (RS 501.6)
- Loi sur l'armée et l'administration militaire (LAAM; RS 510.10)
- Ordonnance concernant l'état-major du Conseil fédéral Division Presse et Radio (RS 510.109)
- Décision du Conseil fédéral du 27 août 1980 : Vorbereitung der Radioversorgung in Katastrophen-, Krisen- und Kriegsfällen (VRK) (préparation de la desserte radio en cas de catastrophes, de crises ou de guerres)
- Ordonnance concernant la réquisition (RS 519.7)
- Ordonnance concernant l'exemption du service militaire (RS 511.31)
- Ordonnance du DDPS sur l'organisation de l'armée (RS 513.111), art. 17, al. 5 : Incorporation des militaires travaillant chez Swisscom dans les formations de la brigade Telecom
- Ordonnances concernant les tâches et l'obligation de service de la brigade télécom 40
- Ordonnance sur la protection civile (OPVi; RS 520.11), chapitre 2 : Transmission de l'alarme à la population et diffusion des consignes sur le comportement à adopter, chapitre 9 : Réseaux de transmission (art. 66 ss.)
- Ordonnance sur la Centrale nationale d'alarme (RS 732.34), art. 5, al. 1, let. a : Collaboration avec la SSR.

3 Exigences de sécurité

3.1 Généralités

Les situations particulières et extraordinaires sont caractérisées par le fait que dans certains secteurs, les processus administratifs normaux ne suffisent plus à résoudre les problèmes et à relever les défis. Ce type de situation exige que les moyens soient concentrés et les procédures simplifiées. Toutefois, les pouvoirs publics sont obligés de continuer à accomplir l'ensemble de leurs tâches. Garantir l'infrastructure nécessaire est donc une exigence essentielle, la même qui s'applique en temps normal. Certains organes responsables de tâches publiques telles que la police, l'armée, la protection de la population et les forces de sauvetage sont particulièrement mis à contribution lors de situations extraordinaires; la disponibilité et la confidentialité des moyens mis en œuvre sont pour eux d'une importance capitale dans le cadre de la gestion de crises. A cela s'ajoute que la situation de crise entraîne en elle-même un besoin d'information et de communication nettement plus important qu'en temps normal. Dans ce contexte, l'information est un instrument de gestion essentiel. Par ailleurs, le besoin d'information de la population s'accroît également lors de situations extraordinaires. Il s'agit ici de respecter notamment le droit constitutionnel de la liberté d'information, qui selon une nouvelle tendance donne droit au citoyen dans une mesure limitée à l'information des autorités.[13] Afin de pouvoir remplir ces exigences, il est indispensable pour les unités d'organisation de disposer d'infrastructures de télécommunication et de radiodiffusion extrêmement sûres.

Il est clair qu'une sécurité absolue n'est souvent pas possible ou du moins pas réaliste, principalement pour des raisons techniques mais également du point de vue économique. La question de la sécurité est donc toujours liée à celle du risque résiduel, c'est-à-dire le risque que l'on accepte volontairement ou que l'on ne peut pas exclure. Pour cette raison notamment, il est absolument indispensable de disposer d'une vue d'ensemble des interdépendances et des dangers concrets.

[13] Voir également ATF 107 Ia 304. Par ailleurs, les art. 10 et 34 de la loi sur l'organisation du gouvernement et de l'administration (LOGA; RS 172.010) fixent une obligation d'information de la part du Conseil fédéral et de l'administration vis-à-vis du public.

3.2 Détails

L'exigence de sécurité est toujours liée à un équipement en particulier. Nous l'avons vu, cette exigence, très élevée, a tendance à augmenter encore lors de situations de crise. Les pages suivantes indiquent par quelles infrastructures (réseaux) les différents organes actifs en situation de crise sont concernés concrètement, et qui exploite ces infrastructures.

Il est essentiel de savoir que dans le cadre de la gestion de crises, la communication entre les différentes instances ne peut être garantie que par les réseaux publics fixes et mobiles. Ces raccordements constituent la base de la communication de tous les organes concernés (armée, protection civile, police, organes de milice, direction civile). Afin qu'ils puissent continuer à fonctionner en situation de crise et en cas de surcharge des réseaux, ils obtiennent la priorité dans les réseaux publics du fournisseur de service universel.

Administration fédérale en général :

Description	Propriétaire/exploitant	Remarques
Réseau de base pour la communication dans l'administration fédérale KOMBV 1-3	Swisscom, Confédération (OFIT)	
Réseau de téléphonie mobile	Swisscom, à l'avenir év. aussi Orange, Sunrise, 3G Mobile	Il est possible aujourd'hui de fixer des priorités dans les réseaux Swisscom.
POLYCOM	Confédération, cantons	Réseau de radiocommunication de sécurité et de sauvetage (modes cellulaire et direct)
Fournisseurs internet	Divers	
Réseaux de radiodiffusion en général (SSR et autres diffuseurs privés)	Swisscom (en général pour la diffusion terrestre des programmes radio de la SSR et de 98 % des programmes de télévision) ainsi que d'autres exploitants privés, EUTELSAT (société française) pour la diffusion par satellite, opérateurs de réseaux câblés (entreprises de CATV) pour la diffusion sur des lignes.	Art. 6 LRTV (sécurité publique, obligation de diffuser) Depuis la CENAL, il est possible d'interrompre les programmes de la SSR pour diffuser des avertissements et des alarmes.

Affaires étrangères :

Description	Propriétaire/exploitant	Remarques
KOMBV4	Swisscom, exploitants étrangers	
Téléphonie mobile	Swisscom, exploitants étrangers	
Réseau radio d'ambassade	Confédération (DFAE et DDPS)	Radiocommunication sur ondes courtes Liaison au ComCenter DFAE par les raccordements AF et Tranet (réseaux militaires)
Liaisons par satellite	INMARSAT (société britannique)	Participation de Swisscom 3 %
Radio ondes courtes (SRI-SSR)	Swisscom sur mandat de SRI-SSR, exploitants étrangers	(Swiss Radio International), information aux Suisses de l'étranger et au personnel du DFAE
Télévision par satellite	Swisscom sur mandat de SRI-SSR, exploitants étrangers	Information aux Suisses de l'étranger et au personnel du DFAE

Armée :

Description	Propriétaire/exploitant	Remarques
Réseau AF	Confédération (DDPS), Swisscom	Réseau général de conduite (réseau fixe et à faisceau hertzien) de la Confédération avec intégration des cantons
BBUS-faisceau hertzien **BBUS-câble**	Confédération (DDPS) Confédération (DDPS) / Swisscom	Transmission opérative par faisceau hertzien Transmission opérative par câble
IMFS et réseaux radio tactiques	Confédération (DDPS)	Exigent l'intervention de troupes de transmission
TRANET	Confédération (DDPS)	Réseau de communication de données de l'armée et de certaines parties de l'administration militaire
VULPUS Radio / VULPUS Télématique	Confédération (DDPS)	

VRK-OUC 77	Propriété :
	- Bâtiments et infrastructure : Swisscom
	- Installations de transmission : Etat-major CF DIPRA
	Exploitation :
	- En situation normale :
	  - Partie civile : Swisscom sur mandat de la SSR
	  - Partie VRK : Swisscom sur mandat de l'Etat-major CF DIPRA
	- En situation extraordinaire :
	  - Swisscom sur mandat de la CENAL
	  - Dès mobilisation : Tc Br 40 sur mandat de l'Etat-major CF DIPRA (Info Rgt 1)
		Desserte radio de la population lors de situations extraordinaires. Fonctionnelle dès que les abris sont occupés, dotée d'une puissance d'émission renforcée.
		Subsidiarité
		(actuellement encore à l'examen)

Protection civile :

Description	Propriétaire/exploitant	Remarques

VRK-OUC 77	Propriété :
	- Bâtiments et infrastructure : Swisscom
	- Installations de transmission : Etat-major CF DIPRA
	Exploitation :
	- En situation normale :
	  - Partie civile : Swisscom sur mandat de la SSR
	  - Partie VRK : Swisscom sur
		Desserte radio de la population lors de situations extraordinaires. Une fois occupés, abris dotés d'une puissance d'émission renforcée.

	mandat de l'Etat-major CF DIPRA - En situation extraordinaire : - Swisscom sur mandat CENAL - Dès mobilisation : Tc Br 40 sur mandat de l'Etat-major CF DIPRA (Info Rgt 1)	Subsidiarité (actuellement encore à l'examen)
INFRANET	Swisscom	Réseau de sécurité pour la transmission de données, toujours prêt à l'utilisation Réseau pour le déclenchement des sirènes stationnaires commandées à distance SFI 457

Police :

Description	Propriétaire/exploitant	Remarques
VULPUS Télématique	Confédération (DDPS), Swisscom	
WAN DFJP	Confédération, Swisscom	
Intranet CCPCS	Confédération, cantons, Swisscom	
Janus-Intranet	Confédération, cantons, Swisscom	
Liaisons internationales		

Approvisionnement économique du pays :

Description	Propriétaire/exploitant	Remarques
Réseaux publics fixes et mobiles	Swisscom, à l'avenir év. aussi Orange, Sunrise, 3G Mobile	Dans les réseaux Swisscom (KWT ou NATEL D Plus), des raccordements peuvent recevoir la priorité
Liaisons par satellite	INMARSAT	Liaisons avec les navires en haute mer
Liaisons sur ondes courtes	Swissradio	Liaisons avec les navires en haute mer en cas de panne des liaisons satellite

Cantons :

Description	Propriétaire/exploitant	Remarques
POLYCOM	Confédération, cantons	Réseau radio de sécurité et de sauvetage (modes cellulaire et direct)
Réseaux d'administration	plusieurs	Réseaux régionaux au sein du système global
Réseaux de gestion du trafic	Cantons et autres	Spécialement pour le réseau national des routes

Organisations civiles de sauvetage :

Description	Propriétaire/exploitant	Remarques
Réseaux publics fixes et mobiles	Swisscom, à l'avenir év. aussi Orange, Sunrise, 3G Mobile	Dans les réseaux Swisscom (KWT ou NATEL D Plus), des raccordements peuvent recevoir la priorité
POLYCOM	Confédération, cantons	Réseau radio de sécurité et de sauvetage (modes cellulaire et direct)

Cette présentation montre que les instances concernées exploitent elles-mêmes les infrastructures de communication dont elles ont besoin, ou alors les font exploiter par un fournisseur de services. Les prestations préalables nécessaires à la fourniture de services de communication sont parfois assurées par des entreprises privées (p.ex. location de capacités de transmission ou d'emplacements qui sont utilisés pour exploiter un réseau de transmission).

4 RISQUES ET MESURES

En règle générale, les infrastructures de communication sont sans cesse exposées à certains risques. Même en situation ordinaire, les exploitants de réseaux doivent prendre des mesures de sécurité de vaste envergure. Comme le montre l'exploitation actuelle, ces mesures sont fort efficaces et la disponibilité des infrastructures en Suisse très grande. Pour les situations extraordinaires toutefois, il a été procédé ci-dessous à une analyse des risques dans les grandes lignes. Il reviendra ensuite aux entités concernées d'opérer une analyse plus détaillée, qui devra être régulièrement actualisée.

4.1 Méthode utilisée pour l'analyse des risques

Pour les besoins du présent rapport, la méthode suivante a été choisie. Il a tout d'abord fallu identifier les risques possibles afin d'évaluer leur degré de probabilité et les dommages qu'ils peuvent générer. Le risque est donc calculé par rapport à sa probabilité de concrétisation et aux dommages qui pourraient survenir dans une situation extraordinaire. En revanche, il n'est pas tenu compte de la probabilité qu'une telle situation se présente. Par ailleurs, il convient de souligner que cette estimation prend en considération des mesures déjà concrétisées permettant souvent de désamorcer le danger et donc de réduire l'urgence de la situation.

Chaque danger a ensuite été classé dans un tableau des risques. Cette représentation graphique regroupe les dangers en fonction de leur gravité et indique la nécessité des mesures que l'Etat *devrait* encore prendre.

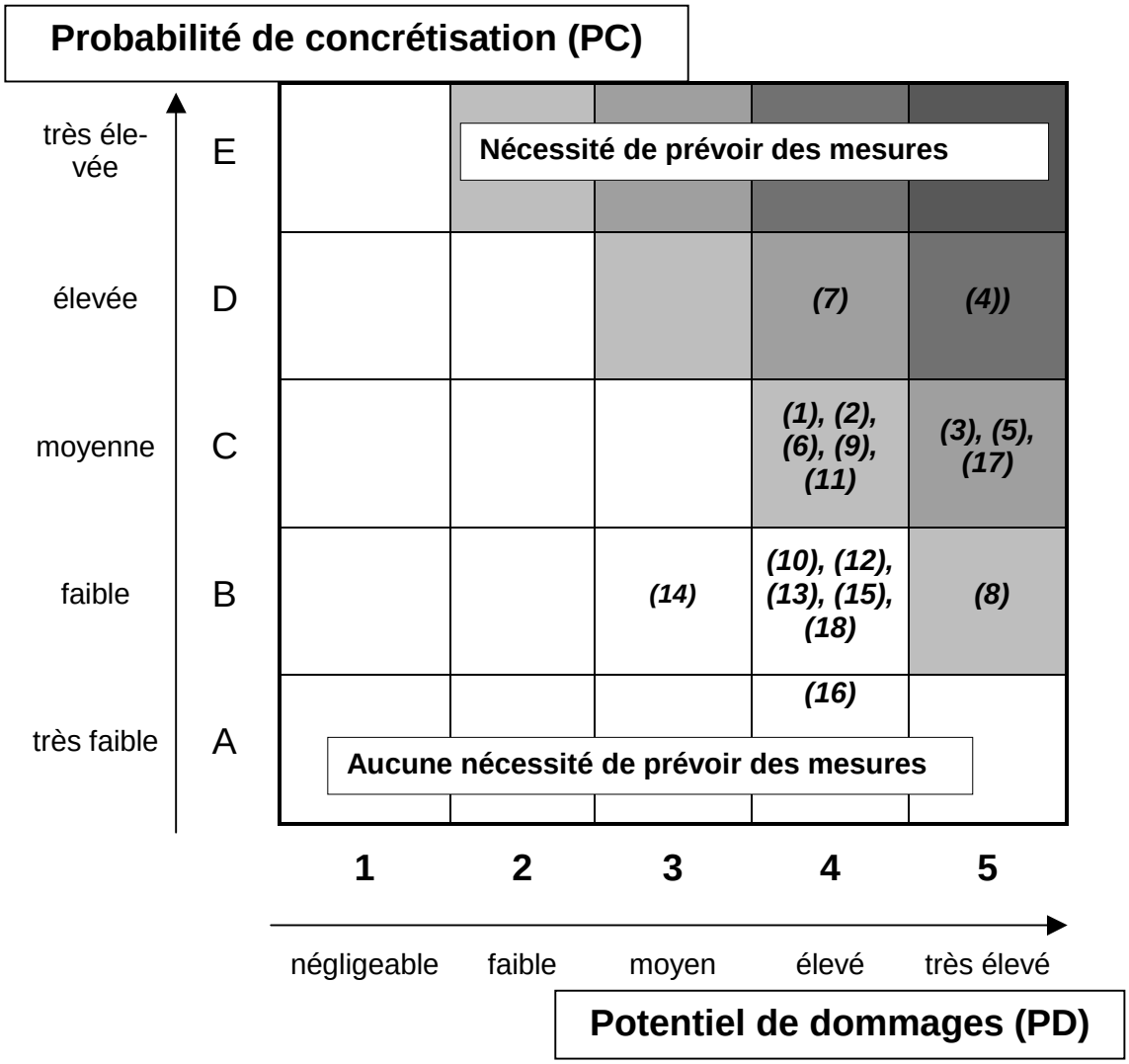

Illustration 1: Tableau des risques (les numéros figurant dans ce tableau correspondent aux risques décrits au chiffre 4.2.:

(1) Surcharge du réseau, (2) Points critiques et réseaux intelligents centralisés, (3) Développement technologique, (4) Technologies étrangères, (5) Centres d'exploitation de réseaux à l'étranger, (6) Technologie par satellite, (7) Problèmes de réception, (8) Privatisation, (9) Fragmentation des entreprises, (10) Internationalisation, (11) Personnel, (12) Sabotage, (13) Panne d'énergie, (14) Catastrophes anthropiques, (15) Catastrophes naturelles, (16) Manque de compatibilité, (17) Problèmes dans le domaine VRK-OUC 77 (18) Monoculture technique.)

La présente analyse ne prétend pas parvenir à une exactitude scientifique absolue, mais elle permet aux experts qui l'utilisent d'identifier les cas où une intervention de l'État est nécessaire.

4.2 Analyse des risques et mesures nécessaires

Les dangers potentiels sont évalués ci-dessous en fonction de la méthode précitée, de même que sont indiquées les mesures qui pourraient être prises. Il existe cinq catégories de dangers, à savoir ceux liés à la technique, au personnel, à la branche IT, aux influences extérieures et à l'organisation.

4.2.1 Dangers liés à la technique

Il s'agit de risques directement liés à la technique sur laquelle est basée l'infrastructure.

4.2.1.1 Surcharge du réseau *(1)*

Description: Une surcharge peut provoquer des pannes temporaires de réseau.

Évaluation: Pour des raisons d'ordre économique, les exploitants de réseaux s'efforcent eux-mêmes d'accroître la capacité de leur réseau aux heures de grand trafic. L'expérience montre cependant que des surcharges peuvent se produire lors de situations extraordinaires. L'art. 48 LTC (voir aussi art. 71 s. OST) autorise la restriction des télécommunications (définition des priorités) lors de situations extraordinaires, ce qui signifie que les usagers prioritaires peuvent avoir accès aux réseaux concernés. Il convient d'examiner l'attribution de priorités aux télécommunications de l'ensemble du réseau dans le cadre de l'interconnexion.

La pratique (cas des inondations à Brigue le 24 septembre 1993) a en outre montré qu'un appel officiel des autorités à téléphoner le moins possible peut s'avérer tout à fait efficace.

En cas de restriction des télécommunications, la loi prévoit d'indemniser les personnes concernées, mais elle ne donne que peu de détails à ce sujet.

Tableau des risques: Probabilité de concrétisation (PC) moyenne, Potentiel de dommages (PD) élevé.

Mesure: Obliger les exploitants de réseaux publics importants (réseau fixe, réseau mobile, réseau IP), à offrir la possibilité d'accorder la priorité à certains groupes de clients et de garantir ces priorités dans le domaine de l'interconnexion. En outre, la question de l'indemnisation doit être réglée de manière plus claire.

4.2.1.2 Points critiques et réseaux intelligents centralisés *(2)*

Description: Les points critiques sont surtout des interfaces non redondantes connectées au réseau ou des voies de câbles passant par un chemin très étroit. En raison du progrès technique et d'une certaine rationalisation, il existe une tendance à diriger le réseau au moyen de serveurs centraux non redondants ou pas suffisamment redondants.

Évaluation: Des points critiques surgissent partout où les communications passent par un petit nombre d'interconnexions de réseau, voire par les mêmes voies de câbles. Les interfaces d'interconnexion entre fournisseurs de services de télécommunication ou entre réseaux mobiles et fixes sont particulièrement concernées. Une panne des interfaces d'interconnexion toucherait à chaque fois tous les clients d'un fournisseur qui souhaitent communiquer avec les clients d'autres fournisseurs. Les dommages causés aux voies de câbles (p.ex. le tunnel du Gothard) dans lesquelles passent les lignes de plusieurs fournisseurs pourraient engendrer une panne simultanée des réseaux de divers fournisseurs importants. Dans le cas des Pays-Bas, on sait par exemple que la panne d'un seul nœud serait problématique pour l'ensemble du raccordement à l'internet du pays tout entier.

Comme le montrent les expériences récentes, la défaillance d'un serveur central peut entraîner une panne de tout le réseau, notamment lorsque la redondance de ce système n'est pas assez prise en compte.

La même problématique existe dans le secteur de la radiodiffusion, par exemple lorsque des exploitants de réseaux câblés prévoient de diffuser les programmes du service universel exclusivement par satellite, sans même posséder d'approvisionnement redondant en énergie.

Tableau des risques: PC moyenne, PD élevé.

Mesures: Dans les concessions, imposer des prescriptions concernant la disponibilité. Prévoir une obligation de déclarer et, par conséquent, recenser les éléments de réseau non re-

dondants dans le descriptif de réseau de la concession, - également lors de l'enregistrement pour les fournisseurs soumis à l'obligation d'annoncer.

4.2.1.3 Développement technologique *(3)*

Description: Le développement technologique démode les systèmes, jusqu'à ce que ceux-cii ne puissent plus être utilisés, faute d'être compatibles.

Évaluation: Le domaine ICT se développe à une vitesse fulgurante. Il est soumis à une véritable pression (technique et économique) à suivre l'évolution technique. Il faut sans cesse augmenter la capacité des systèmes ou même les remplacer, un problème auquel les responsables sont confrontés même en situation ordinaire. Les conditions de base de la disponibilité des infrastructures en situations extraordinaires sont ainsi créées. Il y a peu de risque que des systèmes se montrent surannés lors de situations extraordinaires. Les systèmes les plus en péril sont donc ceux utilisés exclusivement ou principalement en cas de situations extraordinaires (p.ex. l'infrastructure VRK-OUC 77). En effet, il peut arriver qu'ils aient été négligés en temps normal et qu'ils ne soient donc plus disponibles, ou en partie seulement, lors de situations extraordinaires.

A noter que les exploitants de réseaux exposés à la concurrence sont soumis à une grande pression économique sur le plan de la mise à jour de leur réseau.

Il est positif que les technologies gagnent en sécurité au fur et à mesure de leur évolution. Toutefois, en raison des possibilités techniques et des mesures de rationalisation, ce progrès conduit notamment à une centralisation de l'intelligence, qui est à son tour source de risques (voir 4.2.1.2).

Tableau des risques: PC moyenne, PD très élevé.

Mesures: Sensibiliser les responsables.

4.2.1.4 Technologies étrangères *(4)*

Description: Dépendance par rapport à des technologies dont la Suisse ne dispose pas.

Évaluation: Il s'agit là d'une dépendance à prendre très au sérieux, car le potentiel de risques est élevé aussi bien sur le plan de la probabilité de concrétisation que sur celui de l'ampleur des dommages. La balance commerciale de la Suisse est négative dans tous les segments de produits du secteur ICT. Il y a donc une forte dépendance de la Suisse par rapport à l'étranger, qui peut être utilisée abusivement pour exercer une pression politique ou économique sur la Suisse ou sur les sociétés implantées en Suisse. Le fait que les technologies en question sont actuellement importées surtout de pays bien disposés à l'égard de la Suisse est une maigre consolation. En cas de situations extraordinaires, cette problématique ressort en particulier dans le domaine de l'acquisition de pièces de rechange ainsi que parfois au niveau du "second level support", voire souvent sur le plan du "third level support". En raison des progrès techniques fulgurants, un stockage tel qu'il est pratiqué dans d'autres secteurs de l'approvisionnement économique du pays semble peu prometteur, tandis que la mise en place d'une industrie autosuffisante est carrément irréaliste. Tableau des risques: PC élevée, PD très élevé.

Mesures: Stocker n'est guère possible. Établir un engagement contractuel avec les fournisseurs (difficilement réalisable en situations de crise).

Il faut être prêt ici à accepter un risque supérieur à la moyenne.

4.2.1.5 Centres d'exploitation de réseaux à l'étranger *(5)*

Description: Lorsque les centres d'exploitation de réseaux se trouvent exclusivement à l'étranger, la commande de l'exploitation depuis la Suisse n'est pas garantie du tout ou n'est pas garantie dans un délai raisonnable.

Évaluation: Il s'agit d'un phénomène lié d'une part à l'internationalisation des marchés et d'autre part aux processus économiques de rationalisation. Cette situation génère une dépendance à ne pas sous-estimer, car dans un cas extrême, des réseaux de l'étranger pourraient être mis hors service simplement en appuyant sur un bouton. Tableau des risques: PC moyenne, PD très élevé.

Mesures: Soumettre les fournisseurs à l'obligation légale d'aménager en Suisse des centrales locales minimales d'exploitation de réseaux ainsi que des outils de gestion de réseaux qui puissent être utilisés en tout temps de manière autonome par du personnel travaillant en Suisse.

4.2.1.6 Technologie par satellite *(6)*

Description: Dépendance par rapport à des satellites (étrangers).

Évaluation: Cette technique est utilisée notamment pour la distribution de programmes radiodiffusés ou pour la téléphonie (p.ex. navigation en haute mer). La Suisse ne dispose d'aucun satellite propre et, comme le montre l'expérience, la disponibilité des satellites étrangers n'est absolument pas garantie lors de crises internationales. Il s'agit donc d'une situation de totale dépendance, même si la technique par satellite n'a pas été beaucoup utilisée jusqu'ici lors de situations extraordinaires, excepté pour la navigation en haute mer et les représentations suisses à l'étranger. C'est en effet dans ces cas-là que les radiocommunications par ondes courtes ont été considérées comme une solution de rechange. Celle-ci n'est toutefois plus incontestée dans le secteur de la navigation en haute mer, principalement pour des raisons économiques. Tableau des risques: PC moyenne, PD élevé.

Mesures: Garantir d'autres solutions (technique OUC en partie douteuse). Il convient ici de tenir compte d'un certain risque résiduel supérieur à la moyenne.

4.2.1.7 Monoculture technique *(18)*

Description: Force est de constater que, dans la branche TIC (télécommunications-informatique), les fournisseurs sont toujours moins nombreux et qu'ils produisent toujours plus d'infrastructure (matériel informatique et logiciels).

Évaluation: D'une part, les monocultures techniques peuvent rendre des branches entières de l'administration dépendantes d'un seul fournisseur. Il y a ici un problème similaire à celui lié à la dépendance par rapport à l'étranger, décrit au chiffre 4.2.1.4. D'autre part, la situation risque aussi de favoriser la distribution de composants défectueux. La question devient véritablement problématique lorsque l'infrastructure inadéquate ne peut plus être remplacée. A noter que cette tendance à la monoculture découle principalement de la supériorité technique de certains produits. Tableau des risques: PC faible, PD élevé.

Mesures: Aucune mesure nécessaire.

4.2.1.8 Problèmes de réception *(7)*

Description: Des insuffisances techniques chez les destinataires externes à l'administration empêchent le flux d'informations (notamment les habitudes des auditeurs dans le domaine de la radiodiffusion, la non-disponibilité des appareils de réception portables).

Évaluation: Les destinataires concernés ne sont le plus souvent pas conscients de cette problématique. De plus, il existe une grande dépendance par rapport aux exploitants CATV. Tableau des risques: PC élevée, PD élevé.

Mesures: Sensibiliser les milieux de la population concernés.

4.2.2 Branche informatique

La libéralisation des marchés concernés a entraîné de profondes modifications des structures économiques qui influencent également le comportement des agents économiques.

4.2.2.1 Privatisation *(8)*

Description: Jusqu'en 1998, il revenait à l'entreprise étatique des PTT de mettre à disposition l'infrastructure de réseau. Suite à sa privatisation et à l'ouverture des marchés à d'autres fournisseurs, la situation s'est modifiée de manière fondamentale. Désormais, les sociétés privées prennent naturellement leurs décisions en fonction de critères d'économie privée et non pas selon des critères politiques de sécurité.

Évaluation: En tant qu'actionnaire majoritaire – situation prévue par la loi -, la Confédération a eu jusqu'ici une influence considérable sur la politique commerciale de Swisscom, même si elle doit tenir compte de façon adéquate des intérêts des actionnaires minoritaires, conformément aux conditions du régime juridique des sociétés anonymes. Pour d'autres exploitants de réseau, il n'en va pas de même. Cet état de fait a cependant une grande importance pour Swisscom, étant donné que celle-ci continue d'exploiter la plus grande partie de l'infrastructure (télécommunications et radiodiffusion) et, par conséquent, des installations indispensables à l'information et à la communication lors de situations extraordinaires.

En vertu de l'art. 47 LTC, les exploitants d'infrastructures de télécommunication importantes au niveau national peuvent aujourd'hui déjà, indépendamment de qui est propriétaire de l'infrastructure, être contraints de fournir certaines prestations en cas de situations extraordinaires et de prendre les mesures qui s'imposent. Une telle obligation peut figurer dans des concessions, des contrats ou des décisions, ce qui a d'ailleurs été fait à plusieurs reprises dans le cas de Swisscom. Quant à la réquisition pratiquée dans les situations extraordinaires, elle est réservée. Une telle obligation fondamentale n'a pas encore été prévue dans le domaine de la radiodiffusion, une lacune qui sera comblée dans le cadre des travaux de révision de la LRTV.

Par ailleurs, il ne faut pas oublier que certains exploitants privés de réseaux posent également – dans leur propre intérêt - des conditions en matière de sécurité qui concordent souvent avec les exigences politiques liées à la sécurité.

Tableau des risques: PC faible, PD très élevé.

Mesures: Appliquer de manière conséquente l'art. 47 LTC à tous les exploitants importants d'infrastructures de communication. Actualiser régulièrement les besoins et les négocier avec les fournisseurs de prestations, imposer des conditions si nécessaire. Établir un règlement analogue dans le domaine de la radiodiffusion, resp. étendre l'applicabilité à ce secteur.

4.2.2.2 Fragmentation des entreprises *(9)*

Description: Il s'agit de la fragmentation d'entreprises (concentration sur des affaires clés), qui accomplissaient jusqu'alors toutes les tâches inhérentes à un secteur spécifique (planification, construction, exploitation), en diverses entreprises spécialisées et indépendantes.

Évaluation: La fragmentation d'une société, comme elle est pratiquée chez Swisscom, peut compliquer la coordination des mesures. Tableau des risques: PC moyenne, PD élevé.

Mesures: Prendre en compte de manière conséquente, dans le secteur de la régulation, de telles fragmentations d'entreprises (notamment dans les concessions). Amener les décideurs concernés à adopter une approche de réseau et à penser en commun.

4.2.2.3 Internationalisation *(10)*

Description: La libéralisation des plus grands marchés des télécommunications du monde a entraîné des alliances internationales entre fournisseurs. L'importance économique semble être la nécessité actuelle. Certains craignent que des participations étrangères majoritaires à des exploitations de réseaux indigènes s'opposent aux intérêts suisses en matière de sécurité, d'autant plus que l'Etat devrait pouvoir accéder plus difficilement aux unités étrangères de groupes internationaux qu'aux entreprises nationales.

Évaluation: La mondialisation est un phénomène auquel la Suisse ne peut échapper. Une participation étrangère (même une participation majoritaire) n'est en soi pas une menace pour l'infrastructure des télécommunications et de la radiodiffusion. L'affirmation selon laquelle il s'agit là d'une "vente à l'étranger" est une distorsion de la réalité puisqu'elle suggère en l'occurrence que de l'infrastructure est transférée à l'étranger. De nombreuses sociétés implantées en Suisse sont détenues en majorité par des actions ou autres participations étrangères, sans que cette situation mette en péril la sécurité de leurs activités, et cela même si elles s'occupent de domaines de base comme l'approvisionnement en énergie.

La possibilité de créer à l'étranger un équipement de réserve en prévision d'une situation extraordinaire revêt une importance moindre, étant donné que, pour des raisons de rentabilité, les stocks de rechange auprès des fournisseurs devraient être plutôt restreints.

Certes, une entreprise active au niveau international est davantage soumise aux "offensives" les plus diverses (menées par des régulateurs, des concurrents, des clients, des personnes lésées, etc.) qu'une société présente uniquement sur un marché national. Il serait toutefois exagéré de qualifier cet état de fait de danger pour l'infrastructure de sécurité. A noter également que les grandes sociétés évoluant à l'échelon planétaire sont souvent plus stables.

En règle générale, les groupes internationaux possèdent des filiales nationales se profilant réellement comme des exploitants d'infrastructure. L'entraide judiciaire internationale ainsi que le fait de pouvoir s'imposer en tant qu'autorité également dans un environnement mondial relativisent la problématique de l'internationalisation.

Tableau des risques: PC faible, PD élevé.

Mesures: Aucune mesure nécessaire.

4.2.3 Personnel *(11)*

Description: Il s'agit de la disponibilité de spécialistes disposant du savoir-faire nécessaire pour manier l'infrastructure touchant à la sécurité.

Évaluation: Cette dépendance doit être prise très au sérieux car elle présente un potentiel de risques élevé notamment du point de vue de l'ampleur des dommages. Le savoir-faire pour l'aménagement de l'infrastructure n'est pas prépondérant, car cette dernière est généralement déjà en place lors de situations extraordinaires. Il s'agit bien plus de l'exploitation et de l'entretien des systèmes et des réseaux, des domaines où les responsables du côté des usagers ne possèdent souvent pas assez de savoir-faire et doivent donc recourir à des experts. Or, c'est précisément ces connaissances qu'il devient difficile d'obtenir lors de situations extraordinaires. Si, de surcroît, le savoir-faire provient de l'étranger, alors la situation peut encore s'aggraver suivant le genre de crise.

Par ailleurs, la probabilité de concrétisation, et par conséquent le risque, croît en général proportionnellement à la durée de la crise.

A l'heure actuelle, il n'est pas encore possible d'évaluer à quel point la flexibilité introduite dans le cadre du nouveau droit du personnel de la Confédération améliore les conditions de rémunération des spécialistes (problématique du recrutement).

L'art. 69 OST oblige les fournisseurs de services de télécommunication dont les installations ou les services sont essentiels dans des situations extraordinaires à s'organiser en prévision de telles situations, et notamment à mettre à disposition le personnel nécessaire. En outre, la loi sur l'armée et les ordonnances y relatives réglementent la militarisation de Swisscom également du point de vue du personnel.

Tableau des risques: PC moyenne (croît avec la durée de la crise), PD élevé.

Mesures: Utiliser de manière conséquente - grâce à une incitation notamment financière - la possibilité de procéder à une internalisation des connaissances sur le plan des infrastructures exploitées par la Confédération. En outre, des mesures internes de formation permettent d'améliorer le savoir-faire propre. Enfin, il convient d'envisager l'engagement contractuel d'experts externes et, dans le cadre d'Armée XXI, de garantir la disponibilité du personnel pour la couverture des activités de communication et de radiodiffusion importantes sur le plan national.

4.2.4 Influences extérieures

Il est question ici d'attaques perpétrées par des tiers ou de catastrophes naturelles.

4.2.4.1 Sabotage *(12)*

Description: Il s'agit d'attaques ciblées des infrastructures (physiques ou virtuelles): "hacking", attaques "Denial of Services", endommagement des lignes, virus, perturbations des fréquences, etc.

Évaluation: Une attaque ciblée peut être perpétrée par des tiers, mais aussi par des collaborateurs internes à l'entreprise, aux motifs les plus divers : intérêts économiques ou politiques, désir de vengeance, curiosité, etc. Souvent, les sociétés concernées ne perçoivent pas comme telles les attaques commises par leurs propres employés; quant aux attaques de tiers, elles n'en tiennent compte que lorsqu'il est trop tard. Vu la tendance à la centralisation de l'intelligence du réseau et l'existence de points critiques, certains éléments structurels semblent particulièrement sensibles (voir à ce sujet les explications données au chiffre 4.2.1.2). La plupart de ces actes peuvent aujourd'hui déjà être punis au niveau pénal. On constate qu'en règle général, il s'agit de dangers dont beaucoup de milieux sont parfaitement conscients et contre lesquels des mesures appropriées ont déjà été prises, ou du moins prévues, en maints endroits (firewalls, cryptographie, renforcement des installations sensibles, etc.; voir également à ce sujet au chiffre 1.2 les efforts consentis par l'Etat et l'industrie privée). Tableau des risques: PC faible, PD élevé.

Mesures: Aucune autre mesure nécessaire (hormis les mesures à prendre dans le cadre du concept "Information Assurance").

4.2.4.2 Panne d'énergie *(13)*

Description: Les pannes d'énergie peuvent entraîner l'arrêt de réseaux et de systèmes.

Évaluation: Des pannes d'énergie momentanées et locales ne sont jamais à exclure. Étant donné que la plupart des exploitants doivent être préparés à une telle éventualité (groupes électrogènes de secours), il n'est guère nécessaire d'agir à ce niveau-là. En revanche, une panne d'énergie très étendue pourrait, après peu de temps déjà, avoir des effets dévastateurs sur la société et sur l'Etat. Des mesures efficaces sont déjà prévues sur le plan de l'approvisionnement économique du pays. Tableau des risques: PC faible, PD élevé.

Mesures: Aucune autre mesure nécessaire.

4.2.4.3 Catastrophes anthropiques *(14)*

Description: Catastrophes nucléaires, catastrophes chimiques, graves accidents de la circulation, etc.

Évaluation: Certaines catastrophes anthropiques détruisent également les infrastructures de communication et d'information qui étaient justement nécessaires à maîtriser la crise. Les réseaux fixes semblent ici particulièrement fragiles, même si les réseaux mobiles sont également menacés puisqu'ils dépendent eux aussi en partie des installations terrestres. En règle générale, il y a suffisamment de moyens de radiocommunication dans ce genre de situation (utiliser de préférence le mode direct, et désormais aussi POLYCOM). Tableau des risques: PC faible, PD moyen.

Sur la nécessité d'utiliser les réseaux publics et sur la problématique de la surcharge, voir les explications données au chiffre 4.2.1.1.

Mesures: Aucune autre mesure nécessaire.

4.2.4.4 Catastrophes naturelles *(15)*

Description: Inondations, avalanches, tempêtes, etc.

Évaluation: Certaines catastrophes naturelles détruisent également les infrastructures de communication et d'information qui étaient justement nécessaires pour maîtriser la crise. Les réseaux fixes semblent ici particulièrement fragiles, même si les réseaux mobiles sont également menacés puisqu'ils dépendent eux aussi en partie des installations terrestres. En règle générale, il y a suffisamment de moyens de radiocommunication dans ce genre de situation (utiliser de préférence le mode direct, et désormais aussi POLYCOM). Tableau des risques: PC faible, PD élevé.

Sur la nécessité d'utiliser les réseaux publics et sur la problématique de la surcharge, voir les explications données au chiffre 4.2.1.1.

Mesures: Aucune autre mesure nécessaire.

4.2.5 Organisation

4.2.5.1 Manque de compatibilité (16)

Description: En raison du manque de compatibilité entre les techniques ou du manque d'interfaces normalisées, divers milieux d'utilisateurs risquent de ne pas pouvoir communiquer entre eux.

Évaluation: Le problème est connu depuis longtemps. En vue de l'introduction de POLYCOM (norme Tetrapol), un réseau radio de sécurité et de sauvetage dans toute la Suisse est actuellement mis en place. Il est constitué de nombreux sous-réseaux cantonaux et les cantons peuvent choisir s'ils veulent introduire cette norme et quand ils souhaitent le faire. La Confédération coordonne cette introduction au niveau national (gardes-frontière, armée). Avec les pays voisins, il faut également rechercher des solutions compatibles. Pour l'heure, des appareils radio sont encore échangés là où il n'y a pas de canaux collectifs. Dans le cadre européen également, la norme Tetrapol semble toutefois s'imposer largement auprès des forces de sécurité et de sauvetage. Tableau des risques: PC très faible, PD élevé.

Mesures: Aucune autre mesure nécessaire.

4.2.5.2 Problème dans le domaine VRK-OUC 77 *(17)*

Description: Le domaine VRK-OUC 77 est un système intégré de radiodiffusion terrestre par voie hertzienne fonctionnant par OUC. Il garantit la couverture radio nationale lors de situa-

tions extraordinaires et constitue aujourd'hui le seul moyen de transmission dont dispose le Conseil fédéral pour informer la population dans les abris antiatomiques. Les bâtiments et l'infrastructure appartiennent à Swisscom. Les bases et les consignes légales datent du début des années 80, lorsque les acteurs du marché étaient essentiellement la DIPRA (aujourd'hui l'EM CF DIPRA) et l'ancienne régie PTT.

Bien des choses ont changé depuis la libéralisation du marché et les réorganisations qui en ont résulté, notamment dans le domaine organisationnel (séparation des PTT en La Poste et Swisscom, création de l'OFCOM, nouvelles LTC et LRTV, etc.). Pourtant, la nouvelle répartition des compétences et des responsabilités n'a pas ou pas suffisamment été prise en considération dans la législation. Par ailleurs, il convient désormais de tenir compte de la réorganisation d'Armée XXI.

Nombreux sont les milieux qui émettent des réserves quant à la vente du secteur de la radiodiffusion par Swisscom, déjà envisagée auparavant (voir également à ce sujet 4.2.2.1).

Swisscom conserve pour ainsi dire le monopole de la radiodiffusion terrestre par voie hertzienne.

Évaluation:

- Lacunes de réglementation

Le régime de propriété, l'entretien et l'utilisation des émetteurs VRK-OUC 77 présentent quelques lacunes de réglementation qui existaient en partie déjà avant la libéralisation du marché et généraient de nombreuses zones d'ombre au niveau des responsabilités. Les instances concernées n'avaient pas toujours conscience de cette problématique. Mais dans l'intervalle, la nécessité d'agir a été reconnue. L'EM CF DIPRA, la CENAL, l'OFCOM, Swisscom et la SSR ont mis au point notamment les procédures d'utilisation de l'infrastructure émettrice VRK-OUC 77 par la SSR.

- Vente de l'infrastructure

Il est prévu que Swisscom transfère à une filiale à 100% le secteur de la radiodiffusion avec les émetteurs VRK-OUC 77. Une vente n'est pour l'instant pas à l'ordre du jour, mais elle n'est en tout cas pas exclue à l'avenir. Swisscom s'est d'ailleurs déjà engagé par contrat avec la Confédération (DDPS) à transférer l'exploitation et l'entretien du réseau VRK-OUC 77 à un éventuel acquéreur. Si celui-ci, par manque d'intérêt économique, devait mettre les installations hors service ou en négliger l'entretien, alors la capacité de fonctionnement et la disponibilité opérationnelle lors de situations extraordinaires seraient restreintes ou rendues impossibles. En outre, l'EM CF DIPRA ne pourrait plus assumer ses obligations. Les possibilités d'intervention de la Confédération se limiteraient alors momentanément à des instruments relevant du droit contractuel. Jusqu'à l'entrée en vigueur de la nouvelle LRTV, il manquera l'obligation légale imposée au propriétaire ou à l'exploitant d'émetteurs de maintenir ces derniers opérationnels, ou la possibilité pour la Confédération d'imposer certaines dispositions à l'exploitant de l'installation émettrice VRK-OUC 77, de manière similaire à l'art. 47 LTC (voir chiffre 4.2.2.1).

Tableau des risques: PC moyenne, PD très élevé

Mesures: Combler les lacunes de réglementation (en particulier dans le domaine LRTV/LTC et LAAM) en définissant les nouvelles compétences et en fixant les procédures à suivre. Il convient par ailleurs de garantir que, en cas de vente par Swisscom des activités de radiodiffusion, toutes les obligations en la matière (y compris la confidentialité) passent à l'acquéreur et que la Confédération puisse imposer ses intérêts auprès de cet acquéreur de manière efficace. Créer une disposition analogue à l'art. 47 LTC dans le cadre de la révision de la LRTV (respectivement l'application de l'art. 47 LTC dans le secteur de la radiodiffusion).

4.3 Aperçu des risques et des mesures

Le tableau suivant résume les risques exigeant la prise de mesures et désigne les entités responsables des mesures requises.

Risque	**Mesures**	**Responsabilité**	**Remarques** (notamment les actes législatifs importants)
Surcharge du réseau (4.2.1.1)	• Étudier l'introduction de l'obligation pour tous les exploitants de réseaux fixes et mobiles de pouvoir accorder des priorités • Garantir des priorités dans le domaine de l'interconnexion également • Réglementer la question de l'indemnisation de manière plus claire	• Instances compétentes dans le cadre de la défense générale, en collaboration avec l'OFCOM • Pouvoir réglementaire	OST
Points critiques et réseaux intelligents centralisés (4.2.1.2)	• Édicter des prescriptions concernant la disponibilité • Recenser les éléments de réseau non redondants dans la concession ou dans le cadre de l'obligation d'annoncer	• OFCOM, év. pouvoir réglementaire • OFCOM	• Concessions, év. OST • Descriptif du réseau
Développement technologique (4.2.1.3)	Sensibiliser les responsables	Centres administratifs internes et externes de compétences (DDPS, USIC, OFIT, InfoSurance)	
Technologies étrangères (4.2.1.4)	• Constituer des stocks là où cela s'avère judicieux • Établir un engagement contractuel avec les fournisseurs	• OFIT et instances de support au sein des départements • Exploitants de réseaux	***Le risque résiduel reste supérieur à la moyenne.***
Centres d'exploitation de réseaux à l'étranger (4.2.1.5)	Obliger les exploitants à aménager des réseaux qui puissent être utilisés de manière autonome également depuis la Suisse	• Pouvoirs législatif et réglementaire • Examen du respect des dispositions par l'OFCOM	LTC et ordonnances d'exécution
Technologie par satellite (4.2.1.6)	Garantir d'autres solutions		Technique OUC douteuse pour le moment ***Le risque résiduel reste supérieur à la moyenne.***
Problèmes de réception (radiodiffusion (4.2.1.8)	Sensibiliser les milieux de la population concernés	• EM CF DIPRA • Diffuseurs de programmes	
Privatisation (4.2.2.1)	• Appliquer de manière conséquente l'art. 47 LTC à tous les exploitants importants d'infrastructures de commu-	• Coopération étendue et flexible entre les instances compétentes, en collaboration	• Conditions imposées dans le cadre de l'octroi de

	nication • Procéder à une actualisation conséquente • Effectuer des contrôles sévères • Établir une disposition analogue à l'art. 47 LTC dans le secteur de la radiodiffusion (resp. application de l'art. 47 LTC également dans le secteur de la radiodiffusion)	avec l'OFCOM • Pouvoir législatif	la concession
Fragmentation des entreprises (4.2.2.2)	• Prendre en compte, dans le domaine de la régulation, la fragmentation des entreprises • Amener les décideurs concernés à penser en réseau et en commun	• OFCOM • Instances concernées	• Conditions imposées dans le cadre de l'octroi de la concession
Personnel (4.2.3)	• Prévoir des mesures d'incitation financières ou autres pour obtenir du personnel qualifié • Prendre des mesures générales de formation • Procéder à l'engagement contractuel d'experts externes • Réquisitionner du personnel • Militariser et/ou exempter le personnel astreint au service militaire	• Responsables du personnel au sein de l'administration fédérale • Conseil fédéral • Responsables en matière de marchés publics • Instances compétentes auprès de l'armée	• Établissement de contrats-type • Loi sur l'armée et ordonnances dans le cadre d'Armée XXI
Problémes dans le domaine VRK-OUC 77 (4.2.5.2)	• Combler les lacunes de réglementation en définissant les nouvelles compétences et les procédures à suivre • Transférer les obligations à l'acquéreur en cas de vente de l'infrastructure par Swisscom • Créer dans le domaine de la radiodiffusion une disposition analogue à l'art. 47 LTC (resp. appliquer l'art. 47 LTC dans le domaine de la radiodiffusion)	• Législateur : loi ou ordonnance du Conseil fédéral (examen par l'OFCOM et la DIPRA)	• LRTV, LTC, LAAM, ordonnance concernant l'état-major du Conseil fédéral Division Presse et Radio et ordonnance Br Tc 40

5 SYNTHESE DES RESULTATS

Les technologies de l'information sont indispensables non seulement au développement économique, mais également au bon fonctionnement du gouvernement et de l'administration. Elles sont tout simplement la colonne vertébrale de notre société. Cette dépendance implique des risques et des dangers qu'il ne faut pas sous-estimer.

Lors de situations extraordinaires, les exigences en matière d'information et de communication sont plus élevées. Pour les responsables, l'information est à la fois la base des décisions et un instrument de décision. Quant à la population, elle est encore davantage dépendante de l'information en temps de crise. Par conséquent, la sécurité des infrastructures d'information et de communication est absolument essentielle en cas de situations extraordinaires. Une sécurité absolue n'est toutefois pas possible sur le plan technique ni envisageable sur le plan économique.

Dans ce contexte, il convient de prendre au sérieux les inquiétudes selon lesquelles les intérêts nationaux en matière de sécurité des infrastructures d'information et de communication ne pourraient plus être garantis. Le présent rapport est l'occasion de présenter une vue globale des risques possibles, et de confronter les mesures déjà prises, les mesures prévues ainsi que celles qui sont encore nécessaires.

Le catalogue des événements qui pourraient menacer la sécurité lors de situations extraordinaires est long. Il est important que ces différents dangers soient considérés dans leur globalité, afin que les véritables dépendances et interdépendances en jeu puissent être identifiées.

L'analyse des risques montre que les plus grands dangers nécessitant des mesures ont trait à la dépendance face à la technologie, aux questions d'organisation et à la disponibilité de personnel qualifié.

A cet égard, il faut mentionner le fait que les réseaux nationaux sont extrêmement dépendants de technologies étrangères. C'est toutefois justement dans ce domaine qu'il faudra accepter un risque résiduel supérieur à la moyenne. Il en va de même pour l'utilisation de technologies de télécommunication par satellite dans les secteurs de la navigation en haute mer et des affaires étrangères. L'évolution technologique fulgurante que nous connaissons peut également se retourner contre la sécurité des réseaux si elle n'est pas utilisée à bon escient. Les autres risques de nature technique qu'il faudrait contrer par des mesures adéquates sont les suivants : surcharges de réseaux par manque de capacité, acheminement problématique (voies de transport peu ou pas suffisamment dupliquées) et tendances à la centralisation de l'intelligence des réseaux (un serveur gère la totalité du réseau), ce qui peut mener à une grande fragilité des systèmes. Dans le domaine de la radiodiffusion, il faut également mentionner la problématique de la réception. Dans la mesure où il est possible de les gérer en investissant des moyens raisonnables, ces risques doivent être contrés au moyen de conditions claires fixées dans les concessions ou dans la législation, en opérant ensuite des contrôles. En outre, il faut que les personnes concernées acquièrent une véritable conscience des risques possibles, en fréquentant assidûment des cours de sensibilisation. Connaître le danger est déjà une manière de le contrer.

Par ailleurs, il faut également identifier le risque considérable qui existe sur le plan du personnel. En effet, pour ce qui est de l'exploitation et de l'entretien, les utilisateurs des infrastructures IT dépendent souvent largement du savoir-faire de spécialistes externes, qui ne sont parfois pas disponibles en cas de situation extraordinaire. Cette dépendance face au savoir-faire doit être gérée par le biais de mesures de formation. A long terme, la dépendance face à la technologie pourrait également être maîtrisée dans une certaine mesure. Cela implique l'acquisition, d'une part, de connaissances de base, qui s'ajouteraient à la formation spécialisée de la personne concernée (en particulier hautes écoles et écoles spécia-

lisées, recherche), et d'autre part de connaissances spécialisées dans le cadre de la formation continue (souvent organisée par les entreprises). En outre, l'administration doit de devenir plus attrayante dans le domaine du recrutement de personnel, afin de pouvoir à nouveau acquérir du savoir-faire spécialisé.

Il est clair qu'il faut apprendre à vivre avec cette dépendance face à la technologie et au savoir-faire, mais l'Etat doit engager des mesures adéquates afin de faire reculer au maximum les risques de nature organisationnelle. A cet effet, les lacunes (en matière de responsabilité et de processus) apparues dans la réglementation après la libéralisation dans le domaine des VRK-OUC 77 doivent être comblées.

En revanche, la participation de sociétés étrangères à des entreprises nationales présente moins de risques particuliers puisque ce type d'activités peut être gardé sous contrôle par le biais de conditions imposées aux exploitants. Les risques sont nettement plus aigus dans d'autres domaines tels que la dépendance face à la technologie et au savoir-faire. Du fait de l'internationalisation, il faut toutefois vérifier quelles mesures de régulation garantissent que les réseaux et systèmes vitaux pour la Suisse peuvent être contrôlés depuis le pays en cas de situation extraordinaire, indépendamment du siège des propriétaires.

Dans l'ensemble, on constate qu'aujourd'hui la sécurité des infrastructures de communication lors de situations extraordinaires est largement assurée, grâce notamment aux mesures qui ont déjà été prises. Toutefois, afin de respecter les développements actuels et futurs, il faut optimiser la sécurité en prenant des mesures qui restent économiquement supportables et au besoin en les actualisant et en les complétant. Il paraît primordial de garantir que les prestations devant être offertes par l'exploitant selon l'art. 47 LTC soient définies et bel et bien fournies. Pour cette raison, les entités concernées, et principalement les services compétents en matière de coopération de sécurité, doivent formuler en permanence leurs besoins en matière de conventions et de conditions. Les conventions pourraient être conclues directement entre les demandeurs et les exploitants, qui sont soumis à des conditions fixées par l'OFCOM en tant qu'autorité concédante ou par la législation. Ensuite, les services susnommés doivent vérifier régulièrement que la convention et les conditions soient respectées. Dans le contexte de la révision actuelle de la LRTV, des voix s'élèvent pour demander que des conditions supplémentaires soient ajoutées dans le domaine de la radiodiffusion et dans celui des télécommunications. Il s'agit de créer une disposition semblable à celle de l'art. 47 LTC (ou de prévoir l'applicabilité de l'art. 47 LTC à la radiodiffusion). En outre, les responsables et les décideurs doivent être mieux informés des interdépendances et des risques en matière de sécurité, afin d'acquérir la sensibilité nécessaire pour réagir judicieusement et rapidement face aux dangers. A cet égard, les manifestations telles que l'exercice stratégique INFORMO et l'engagement de la Confédération dans la fondation InfoSurance prennent une importance capitale. Elles permettent en effet un échange de savoir et d'expérience entre l'économie et l'administration.

Enfin, il faut rappeler une fois de plus qu'il n'existe pas de "super-moyen" à même de résoudre tous les problèmes de sécurité. Un concept de sécurité global est une mosaïque composée d'une foule de petits éléments. Par ailleurs, la question qu'il faut se poser est toujours la même : quel risque résiduel peut-on ou doit-on accepter ?