ETAT DE FRIBOURG
STAAT FREIBURG

Organe cantonal de conduite OCC
Kantonales Führungsorgan KFO

Protection de la population
Bevölkerungsschutz

Rte des Arsenaux 16, Case postale 185, 1705 Fribourg

T +41 26 305 30 30, F +41 26 305 30 04,
www.fr.ch/sppam

Plan d'engagement cantonal

—

Panne des réseaux d'information

—

Direction de la sécurité et de la justice **DSJ**
Sicherheits- und Justizdirektion **SJD**

ETAT DE FRIBOURG
STAAT FREIBURG

Organe cantonal de conduite OCC
Kantonales Führungsorgan KFO

Protection de la population
Bevölkerungsschutz

Rte des Arsenaux 16, Case postale 185, 1705 Fribourg
T +41 26 305 30 30, F +41 26 305 30 04
www.fr.ch/sppam

Fribourg, le 25 avril 2017

Panne des réseaux d'information

—

Plan d'engagement

Table des matières

—

Table des illustrations

Tables des abréviations

BCM/BCP	Business continuity management / Business continuity plan[1]
CASU144	Centrale d'appels sanitaires urgents 144
CEA	Centrale d'engagement et d'alarme (112-117-118)
CInfo	Cellule information
CRens	Cellule de renseignement
DFin	Direction des finances
EMCC	Etat-major cantonal de conduite

[1] Management / Plan de continuité

EMF ABCN	Etat-major de conduite fédéral ABCN (atomique-biologique-chimique-naturel)
IC	Infrastructure critique
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
OCC	Organe cantonal de conduite
OCS	Organe de conduite sanitaire
ORCAF	Organisation catastrophe Fribourg
ORCOC	Organe communal de conduite
PCi	Protection civile
SITel	Service de l'informatique et des télécommunications
Spéc	Spécialiste(s)
TIC	Technologie de l'information et de la communication

1. Introduction

Notre société moderne est énormément basée sur les systèmes informatiques et TIC (technologie de l'information et de la communication) - appelés dans le présent plan d'engagement "réseaux d'information" (voir également sous chap. 1.5.1) -. Pour ainsi dire, tous les systèmes de production et de communication sont basés ou utilisent des systèmes informatiques; il est rare de trouver encore un système ne fonctionnant que mécaniquement. De plus, les médias ne peuvent plus informer la population sans informatique, et la population ne peut plus communiquer sans système informatique.

Lors d'une panne de ces réseaux d'information, il est nécessaire de prendre des mesures afin de protéger la population et garantir ses bases d'existence. Dans l'événement, des mesures de conduite concrètes sont alors à prendre afin d'assurer le maintien des réseaux d'information.

Il appartient donc dans le présent plan d'engagement de définir les mesures nécessaires à appliquer avant et durant un tel événement.

1.1. Bases

> Ordonnance du 9 mars 2007 sur la radio et la télévision (ORTV, RS 784.401)
> Loi du 13 décembre 2007 sur la protection de la population (LProtPop, RSF 52.2)
> Loi du 9 septembre 2009 sur l'information et l'accès aux documents (LInf, RSF 17.5)
> Ordonnance du 14 mars 2016 sur la communication en cas d'événement extraordinaire (RSF 52.24)
> Plan ROUGE.

1.2. Buts du plan

Ce plan d'engagement sert à:
> Garantir le même niveau d'information parmi tous les acteurs
> Détecter et identifier une telle situation
> Se préparer à faire face à un tel événement
> Donner au Conseil d'Etat et aux organes de conduite les éléments nécessaires à la conduite de l'événement
> Définir les missions des partenaires
> Limiter les effets
> Définir les actions et les moyens nécessaires à la gestion d'une panne des réseaux d'information
> Définir la collaboration avec les entreprises, et plus particulièrement avec les infrastructures critiques.

1.3. Délimitations

> Le présent plan d'engagement ne traite pas des mesures de prévention.

> Ce plan ne traite que la partie cantonale de la gestion de l'événement, tout en assurant le lien avec la Confédération.

> Les pannes des systèmes informatiques doivent être réglées par les exploitants/propriétaires, c'est-à-dire les entreprises. Elles ne font pas l'objet de ce plan d'engagement.

- La recherche de l'origine d'une panne n'est pas jugée importante pour protéger la population et garantir ses bases d'existence. Elle est intimement liée à la résolution des pannes des systèmes informatiques réglées par les entreprises; elle ne fait donc pas partie de ce plan d'engagement.
- Les conséquences indirectes d'une panne des réseaux d'information (panne électrique, rupture de l'approvisionnement en nourriture….) ne font pas l'objet de ce plan d'engagement. Elles sont réglées selon les plans d'engagement prévus à cet effet (ex: plan d'engagement "Rupture d'approvisionnement électrique").
- Les cellules de crise de l'Etat, qui devront régler une telle panne au sein de "l'entreprise Etat", sont considérées et traitées comme toute autre entreprise.
  - Une panne des réseaux d'information au sein de l'Etat est gérée par le SITel et par conséquent par la cellule de crise de la DFin. Par contre, le SITel est également considéré comme fournisseur TIC, notamment au profit de l'OCC.
- Une panne de la communication entre les échelons de conduite de la Confédération et des cantons (OCC/EMCC) ne sera à 99% plus possible grâce au projet "Réseau de données sécurisé" (RDS). Si toutefois une panne devait survenir, les mesures de communication redondante ou alternative, telles que définies dans ce plan, seraient appliquées.

1.4. Relation avec d'autres plans d'engagement

Ce plan d'engagement est évidemment activé lorsqu'on se trouve dans une situation de panne des réseaux d'information.

Mais il peut également être utilisé lorsque d'autres événements (p. ex. rupture d'approvisionnement électrique) ont comme conséquences une telle panne des réseaux d'information. Il représente dès lors une certaine transversalité et son utilisation dépend alors de la situation.

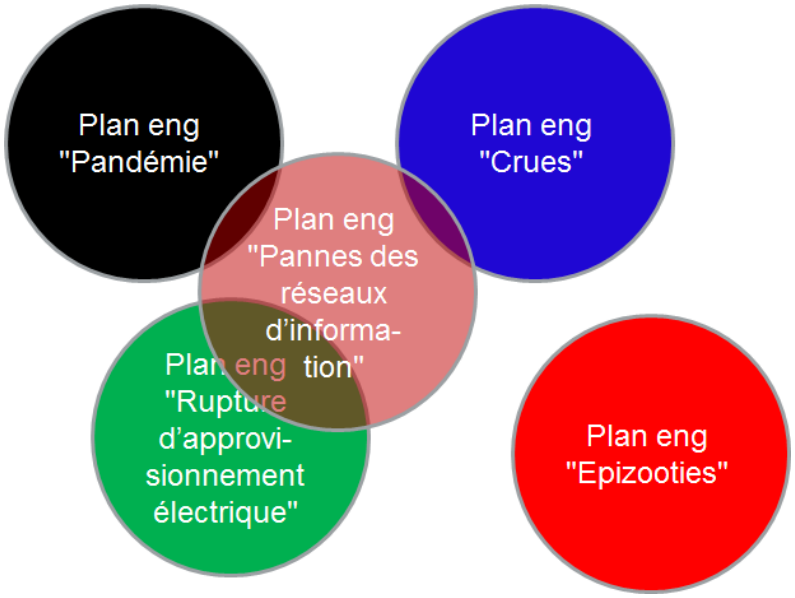

Figure 1: Illustration de la relation avec d'autres plans d'engagement

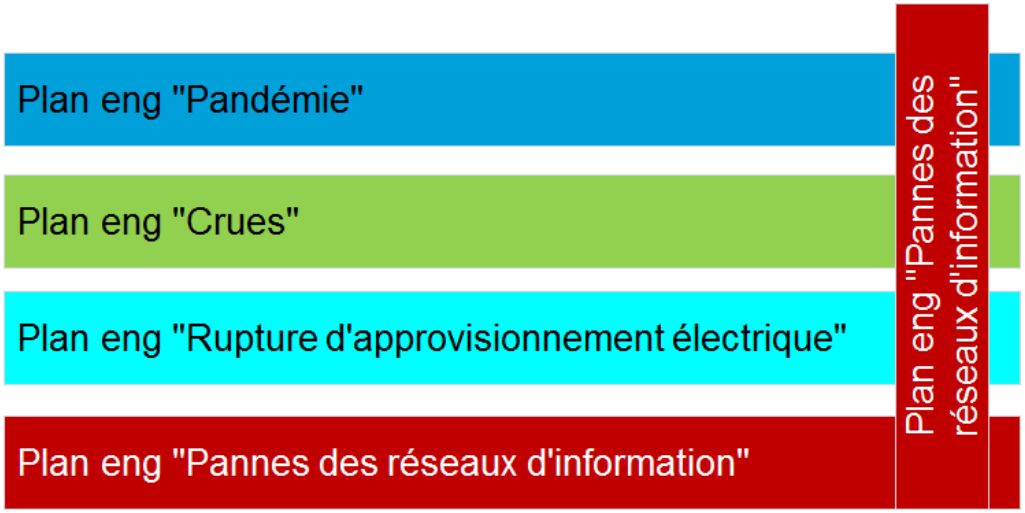

Figure 2: Transversalité du plan d'engagement

1.5. Définitions

1.5.1. Panne des réseaux d'information

On entend par "panne des réseaux d'information":
> La panne des systèmes (producteurs, transporteurs et émetteurs) des **réseaux d'information**
> La panne des réseaux et systèmes **informatiques**

1.5.2. Hors service

Indisponibilité complète d'une machine, d'un appareil, d'un système ou d'un service.

1.5.3. Fonctionnement partiel

Indisponibilité de certains éléments d'une machine, d'un appareil, d'un système ou d'un service.

1.5.4. Identification

Opération par laquelle le système identifie et authentifie un autre système, resp. son origine.

1.5.5. Fausse information

Information erronée, lacunaire, partielle ou non intègre envoyée ou reçue de/par un système.

1.5.6. Vecteur

Ce qui sert de support à la transmission des informations. Parmi les vecteurs, on comprend les systèmes de production, les moyens de transports et les émetteurs/récepteurs.

1.5.7. Information

L'information désigne à la fois le message à communiquer, son format et son contenu.

1.5.8. Systèmes de production

Un système de production regroupe l'ensemble des éléments ou sous-systèmes interconnectés entre eux, matériels et immatériels, ainsi que des processus qui sont nécessaires à la production d'informations.

1.5.9. Moyens de transports

Les moyens de transport regroupent l'ensemble des moyens servant à la transmission d'informations de quelque sorte que ce soit, d'un endroit à un autre, par des technologies, comme par exemple le fil de cuivre, la fibre optique, le laser, la radio, ou la lumière infrarouge.

1.5.10. Emetteurs/récepteurs

Regroupe l'ensemble des moyens techniques, électroniques et humains permettant d'émettre et de recevoir des informations.

1.5.11. Niveaux de la menace

Pour ses messages d'information et d'alerte, MELANI a défini les niveaux de menace ci-dessous:

- **Latent**: La menace n'est pas active en Suisse. Elle est cependant continuellement observée et de nouveaux éléments peuvent conduire à sa réévaluation.
- **Contained**: Des infrastructures d'information critiques en Suisse sont attaquées. En raison des mesures prises, il n'y a cependant pas de dommages.
- **Low**: La menace concerne la Suisse et touche les utilisateurs. Cette menace n'est que modérée pour les infrastructures critiques.
- **Medium**: La menace concerne la Suisse et a un impact fort sur les utilisateurs et les infrastructures critiques.
- **Imminent**: Des infrastructures critiques sont attaquées de manière ciblée, de telle sorte que des fonctions critiques pourraient être menacées.

1.6. Description

1.6.1. Thème

Sous l'angle de la protection de la population, une défaillance des systèmes informatiques et TIC – pour rappel, appelés dans le présent plan d'engagement "réseaux d'information" - a des conséquences directes essentiellement sur l'information interne des organes de conduite et des forces d'intervention, ainsi que sur l'information de la population. Les conséquences indirectes quant à elles sont diverses, car toute défaillance d'un système, vital pour le maintien des conditions d'existence de la population, peut avoir des conséquences dramatiques.

Une défaillance de ces systèmes informatiques et TIC peut également avoir des conséquences considérables, par exemple dans la production de nourriture et d'énergie, ainsi qu'au niveau de l'insécurité de la population. Tout comme l'électricité, il est inconcevable aujourd'hui que les réseaux d'information ne soient plus disponibles.

Non seulement la vulnérabilité de ces réseaux d'information est très grande, mais de surcroît, une défaillance peut survenir soudainement, sans préavis, avec très rapidement de grandes conséquences. Une telle panne avec un impact relativement faible est très probable, alors que la probabilité d'occurrence d'une défaillance, dont les conséquences sont telles qu'elles nécessitent la mise sur pied de l'OCC, est relativement faible.

Finalement, ces systèmes sont tellement interconnectés qu'une défaillance locale et mineure peut avoir des conséquences graves et de grande ampleur ailleurs (effet domino, voire effet papillon[2]).

1.6.2. Eléments principaux[3]

1.6.2.1. Vecteurs

Afin de traiter les différents aspects des réseaux d'information ou de la technologie de l'information et de la communication (TIC), il a été jugé nécessaire de faire la distinction entre les différents vecteurs de cette information. Ainsi figurent parmi les vecteurs d'information retenus:
> les **systèmes de production**,
> les **moyens de transport**
> et les **émetteurs et récepteurs**
de cette information.

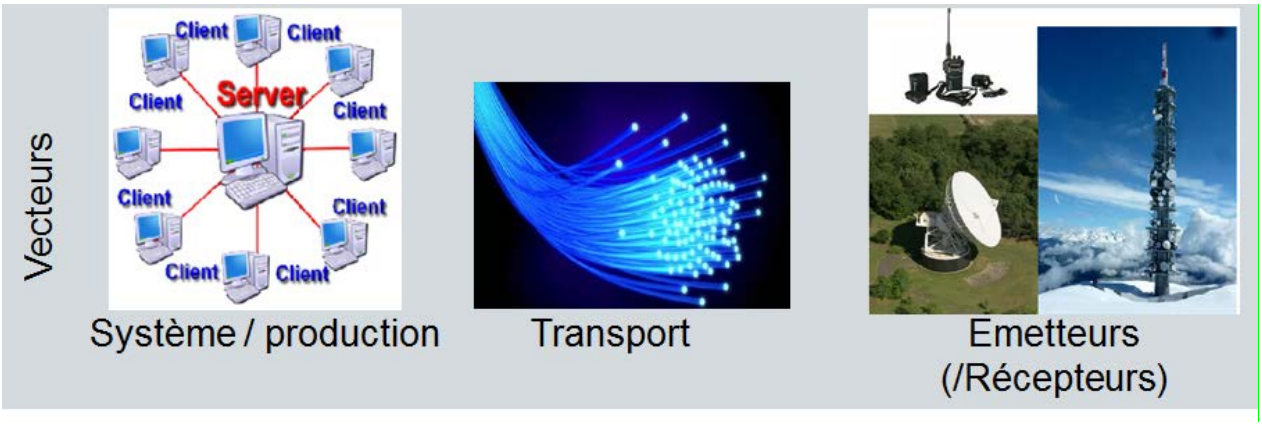

Figure 3: Types de vecteurs

1.6.2.2. Catégories de panne

En cas de panne des réseaux d'information, il importe de distinguer les différentes catégories de panne ci-dessous:
> **Hors service**
> **Fonctionnement partiel**
> **Fausses infos**
> **Identification**

Ces catégories, notamment dans le cadre des éléments déclencheurs (voir sous 2.4), permettent d'apprécier l'importance de la panne et de définir les mesures appropriées.

[2] Effet papillon: Le battement d'ailes d'un papillon au Brésil peut provoquer une tornade au Texas
[3] Voir également les définitions sous 1.5

1.7. Acteurs[4]

Pour faire face à une panne des réseaux d'information, différents domaines ont été identifiés comme acteurs, à savoir:

> **Conseil d'Etat**: il assure la direction politique de l'événement en prenant des décisions de nature politique, en donnant des directions à prendre par l'OCC et en validant ses propositions de mesures.

> **OCC**: il assure la conduite opérationnelle au niveau cantonal, en coordonnant les opérations à l'échelon cantonal. A cet effet, il est renforcé par les spécialistes nécessaires.

> **ORCOC**: ils assurent la conduite opérationnelle au niveau local, en coordonnant les opérations à l'échelon communal. Ils reçoivent les directives nécessaires de l'OCC.

> **Feux bleus**: font partie des feux bleus la police cantonale, les corps de sapeurs-pompiers et les éléments du domaine sanitaire[5]. Ils exécutent dans le terrain les mesures décidées par l'OCC.

> **PCi**: elle est d'une part un élément d'appui aux feux bleus pour assurer la durabilité d'un engagement, d'autre part un élément principal de la remise en état.

> **CInfo**: elle assure la gestion de l'information au profit de l'OCC.

> **SITel**: il assure l'exploitation des réseaux informatiques et téléphoniques ainsi que celle des terminaux de l'Etat.

> **Médias**: ils assurent la transmission des informations à la population.[6]

> **Exploitants des réseaux TIC**: font partie des exploitants des réseaux TIC, les fournisseurs d'accès internet et les opérateurs téléphoniques. Ils assurent l'exploitation des réseaux de communication.

> **Confédération**: par le biais de ses instances spécialisées, elle assure la surveillance de la situation informatique et prend éventuellement des mesures à l'échelle du pays.

1.8. Structure du plan d'engagement

La présente partie principale du plan d'engagement contient les éléments généraux pour faire face à une panne des réseaux d'information. Elle donne à tous les acteurs notamment les lignes directrices de la gestion de l'événement ainsi que les dispositions particulières.

Les éléments concrets de la conduite, notamment les solutions à apporter pour faire face à l'événement, figurent dans les documents de conduite "Matrice des responsabilités" (voir annexe 1) et "Planification de gestion" (voir annexe 2).

---

[4] Ne sont relatés que les acteurs principaux; tous les acteurs, à qui une mission est attribuée dans le présent plan d'engagement, sont énumérés dans la matrice des responsabilités

[5] Conduits par l'OCS

[6] Cette obligation dépend des bases légales auxquelles ils sont soumis; ex: les médias audio-visuels sont soumis à l'ORTV

2. Principes de conduite

2.1. Axes

Le plan d'engagement définit deux aspects des pannes des réseaux d'information auxquels il faut pouvoir faire face:

1. **La surveillance, la détection et l'analyse**
2. **L'impossibilité de communiquer** (interne & externe)

Les autres conséquences d'une panne des réseaux d'information sont gérées par le biais des plans ad hoc (voir remarques au chap. 1.3 "Délimitations").

2.1.1. Surveillance, détection et analyse

La surveillance, la détection et l'analyse de la situation des réseaux d'information s'effectue idéalement par le biais du monitoring (voir sous chap. 2.4). Elles constituent la base pour pouvoir apprécier la nécessité de déclencher le présent plan d'engagement.

2.1.2. Impossibilité de communiquer

Pour faire face à une impossibilité de communiquer à l'interne de l'Organisation catastrophe Fribourg (ORCAF), c'est-à-dire avec/entre les organes de conduite et les formations d'intervention, les mesures principales sont l'utilisation de moyens alternatifs, dont par exemple le basculement sur d'autres réseaux de communication ou l'utilisation de systèmes alternatifs.

Pour informer la population, des moyens alternatifs particuliers seront mis en place, tels que des postes/stands d'information.

2.2. Liens entre les acteurs

Les différents acteurs, tels que mentionnés sous 1.7, interagissent entre eux au niveau de l'échange d'information. Chacun a donc ainsi un rôle à jouer afin que l'OCC dispose d'une image consolidée de la situation.

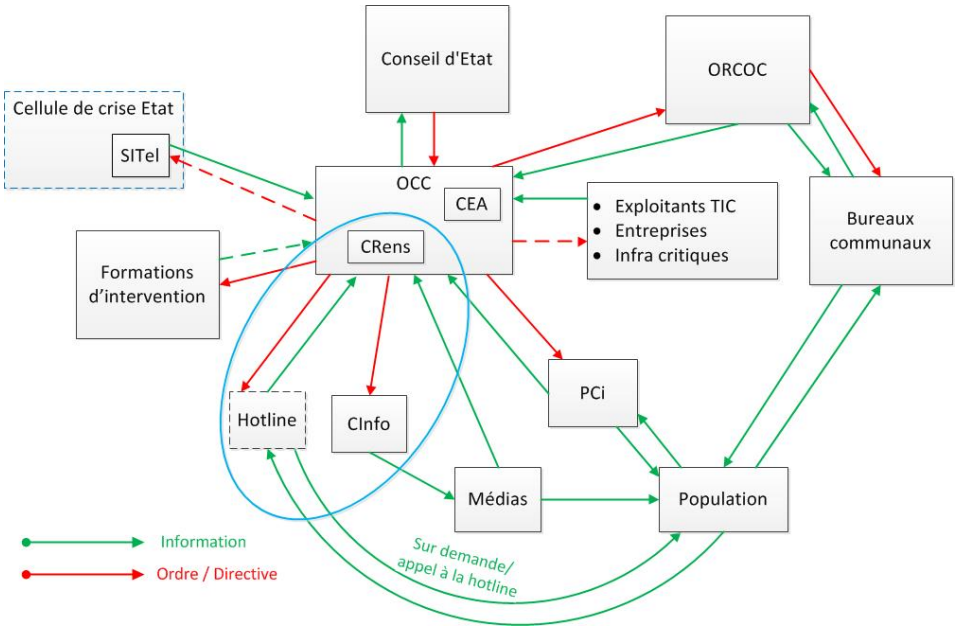

Figure 4: Flux de communication entre les acteurs

2.3. Aspects temporels

En cas de panne des réseaux d'information, il est important pour les organes de conduite:
> D'avoir défini au préalable la durée acceptable de la panne d'un système (**durée admissible d'indisponibilité**)
> De connaître la **durée nécessaire de mise en service** d'une solution alternative.

2.3.1. Durée admissible d'indisponibilité

Ces durées, concernant essentiellement pour les systèmes et prestations critiques, notamment celles des infrastructures critiques, ne peuvent être définies précisément. C'est pourquoi il est préférable de prioriser les infrastructures critiques en fonction de leur importance pour la survie de la population et du maintien de ses conditions d'existence. Pour cela, on se base sur la priorisation de la pyramide de Zufflov (voir ci-dessous). En tenant compte de la criticité des infrastructures critiques et de leur priorité selon Zufflov, la criticité prime (C') donne un bon indicateur sur la priorisation des infrastructures.

A l'engagement, il sera tout de même nécessaire de faire une appréciation de la situation pour chaque infrastructure critique.

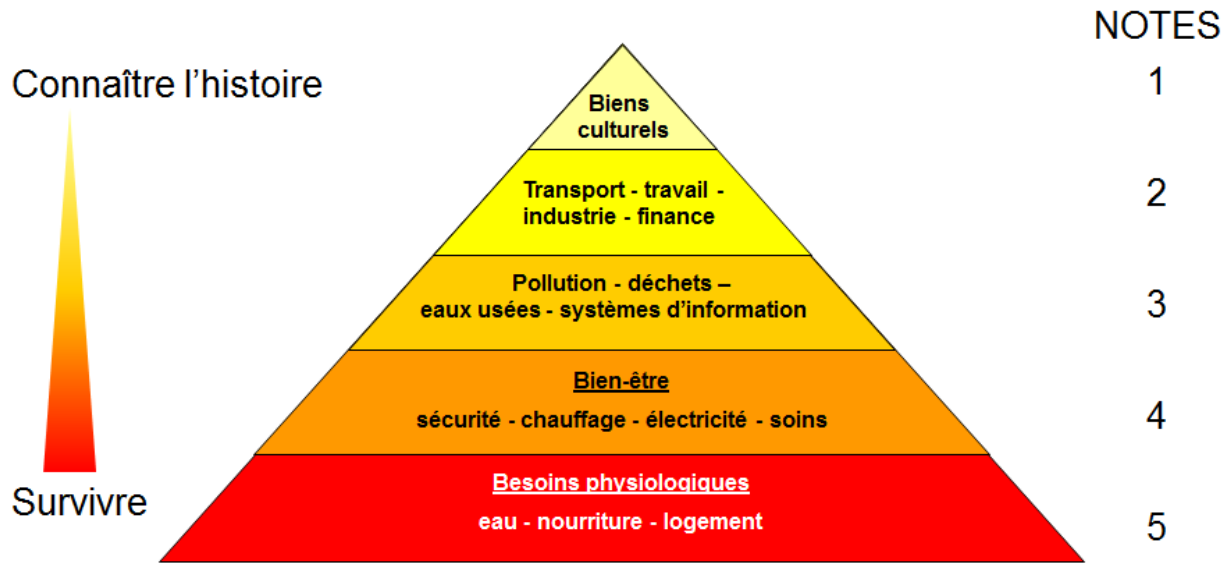

Figure 5: Pyramide de Zufflov

2.3.2. Durée nécessaire de mise en service

En fonction de la situation, notamment de l'urgence des mesures à prendre, il est impératif que les organes de conduite connaissent le temps nécessaire pour mettre en œuvre une mesure. Pour ce faire, les mesures, qui se prennent à l'engagement, ont été complétées avec une estimation du temps de mise en service (voir annexe 2 "Planification de gestion"). Cette estimation étant subjective, elle ne donne qu'une indication du temps nécessaire à la mise en œuvre et il sera nécessaire de la réévaluer à l'engagement.

2.4. Déclencheurs

Alors que la décision finale de déclencher le présent plan d'engagement et les mesures qu'il contient, resp. de mettre sur pied l'OCC pour faire face à un tel événement est en mains du chef

OCC, celui-ci se basera pour ce faire sur les informations reçues du SITel ou de la police cantonale qui assurent un monitoring[7].

Ce monitoring se réalise par une surveillance globale et subjective de la situation, en extrapolant les informations reçues. Le SITel et la police cantonale sont en quelque sorte les indicateurs d'une situation cantonale, resp. que le canton se trouve dans un situation de panne des réseaux d'information.

Ainsi:

> Le **SITel** surveille le réseau de l'Etat et analyse la situation. Sur cette base, et en tenant compte des informations reçues de MELANI, il extrapole cette situation à tout le canton et en fait état à l'OCC[8].

> La **Police cantonale**, notamment sur la base des informations du CEA et de la brigade financière, apprécie la situation et en fait état à l'OCC[8].

3. Missions

Une matrice des responsabilités (voir sous 3.2) et une planification de gestion (voir sous 3.4) ont été établies sur la base de l'appréhension des problèmes[9] qu'une panne des réseaux d'information peut poser. Cette planification a pour but de définir les actions et mesures que chaque acteur doit effectuer, en fonction des phases.

3.1. Solutions

Pour pouvoir faire face aux problèmes identifiés dans l'appréhension du problème, des solutions ont été établies (voir annexe 3). Ce tableau liste, pour chaque vecteur et en fonction de chaque catégorie de panne, les solutions possibles[9]. Celles-ci doivent être appréciées par l'organe de conduite ou la formation d'intervention responsable (voir matrice des responsabilités ci-dessous) quant à leur opportunité d'être mises en œuvre.

3.2. Matrice des responsabilités

La matrice des responsabilités attribue les responsabilités des mesures de préparation, de planification et d'action (voir annexe 1) aux différents acteurs en fonction du rôle qui leur est attribué.

3.3. Missions générales

En complément des missions figurant dans le Plan ROUGE, les acteurs accomplissent les missions générales ci-dessous. Les missions particulières sont détaillées dans la planification de gestion (voir sous 3.4).

3.3.1. Conseil d'Etat

> Valider les mesures proposées par l'OCC
> Répondre aux demandes de l'OCC quant aux dérogations aux règles ordinaires en vigueur, dont notamment relatives à la protection des données et au secret professionnel

---

[7] D'autres solutions de monitoring sont envisageables, comme par exemple un monitoring avec les entreprises
[8] Hors événement à la protection de la population
[9] Liste non exhaustive

3.3.2. OCC

> Etre capable de se mettre sur pied, même en l'absence de moyens de communication
> Etre capable de communiquer à l'interne et avec ses partenaires à l'aide de moyens alternatifs ou sécurisés
> Conduire l'information
> Assurer le lien avec la Confédération

3.3.3. ORCOC

> Etre capable de se mettre sur pied, même en l'absence de moyens de communication
> Etre capable de communiquer à l'interne et avec ses partenaires à l'aide de moyens alternatifs ou sécurisés
> Appliquer les directives de l'OCC.

3.3.4. Police

> Assurer la coordination de l'information des feux bleus
> Analyser le degré de menace informatique du canton et l'annoncer spontanément à l'OCC[10]
> Etre capable de se mettre sur pied, même en l'absence de moyens de communication
> Etre capable de communiquer à l'interne et avec ses partenaires à l'aide de moyens alternatifs ou sécurisés
> Garantir en tout temps les prestations sécuritaires, d'intervention et de sa centrale d'alarme
> Prioriser les activités

3.3.5. Sapeurs-pompiers

> Etre capable de se mettre sur pied, même en l'absence de moyens de communication
> Etre capable de communiquer à l'interne et avec ses partenaires à l'aide de moyens alternatifs ou sécurisés
> Garantir en tout temps les prestations sécuritaires et d'intervention
> Prioriser les activités

3.3.6. OCS

> Etre capable de se mettre sur pied, même en l'absence de moyens de communication
> Etre capable de communiquer à l'interne et avec ses partenaires à l'aide de moyens alternatifs ou sécurisés
> Garantir en tout temps les prestations sanitaires, d'intervention et de sa centrale d'alarme
> Prioriser les activités

3.3.7. PCi

> Etre capable de se mettre sur pied, même en l'absence de moyens de communication
> Etre capable de communiquer à l'interne et avec ses partenaires à l'aide de moyens alternatifs ou sécurisés
> Garantir le déclenchement des sirènes

[10] Hors événement à la protection de la population.

> Au profit des partenaires, mettre en place et assurer l'exploitation de moyens de communication et d'information alternatifs
> Appuyer les partenaires, notamment feux bleus, dans leurs missions

3.3.8. CInfo

> Etre capable de se mettre sur pied, même en l'absence de moyens de communication
> Etre capable de communiquer à l'interne et avec ses partenaires à l'aide de moyens alternatifs ou sécurisés
> Assurer la communication avec la population

3.3.9. SITel

> Analyser la situation informatique de l'Etat ainsi que le degré de menace informatique du canton, et l'annoncer spontanément à l'OCC[11]
> Etre capable de communiquer à l'interne et avec ses partenaires à l'aide de moyens alternatifs ou sécurisés
> Fournir les prestations techniques nécessaires à l'ORCAF

3.3.10. Médias

> Etre capable de communiquer à l'interne et avec ses partenaires à l'aide de moyens alternatifs ou sécurisés
> Prendre toutes les mesures nécessaires afin de garantir leurs prestations

3.3.11. Fournisseurs d'accès / Opérateurs téléphoniques[12]

> Etre capable de communiquer à l'interne et avec ses partenaires à l'aide de moyens alternatifs ou sécurisés
> Prendre toutes les mesures nécessaires afin d'augmenter la résilience de leurs systèmes et de garantir leurs prestations vitales
> Mettre en place des redondances pour les systèmes
> Veiller à ce que leurs systèmes soient en permanence:
  > disponibles
  > fiables
  > sûrs
> Etablir leur BCM/BCP pour faire face à un événement "panne des réseaux d'information"
> Fournir les prestations techniques nécessaires à l'ORCAF
> Informer l'OCC de la résolution de la panne

3.3.12. Exploitants IC

> Prendre les mesures préventives nécessaires pour augmenter la résilience de leurs systèmes et de garantir leurs prestations vitales
> Mettre en place des redondances pour les systèmes vitaux
> Etablir leur BCM/BCP pour faire face à un événement "panne des réseaux d'information"

---

[11] Hors événement à la protection de la population.
[12] Yc. exploitants des réseaux TIC

> Informer l'OCC de la résolution de la panne

3.3.13. Confédération

> Etre capable de communiquer à l'interne et avec ses partenaires à l'aide de moyens alternatifs ou sécurisés
> Fournir les prestations techniques nécessaires à l'OCC

3.4. Planification de gestion

La planification de gestion (voir annexe 2) se construit en trois niveaux:

> Le 1er niveau, intitulé "Actions" est en quelque sorte la mission générale de chaque acteur. Celle-ci donne l'idée de manœuvre générale. Elles sont décrites à l'annexe 4 "Actions – Description".

> Le 2ème niveau constitue la mission particulière de chaque acteur, lui permettant de réaliser l'intention/la mission du 1er niveau.

> Le 3ème niveau de préparation comprend les mesures de planification concrètes. Les différents acteurs apprécient la nécessité et l'opportunité pour leur service de réaliser ces mesures.

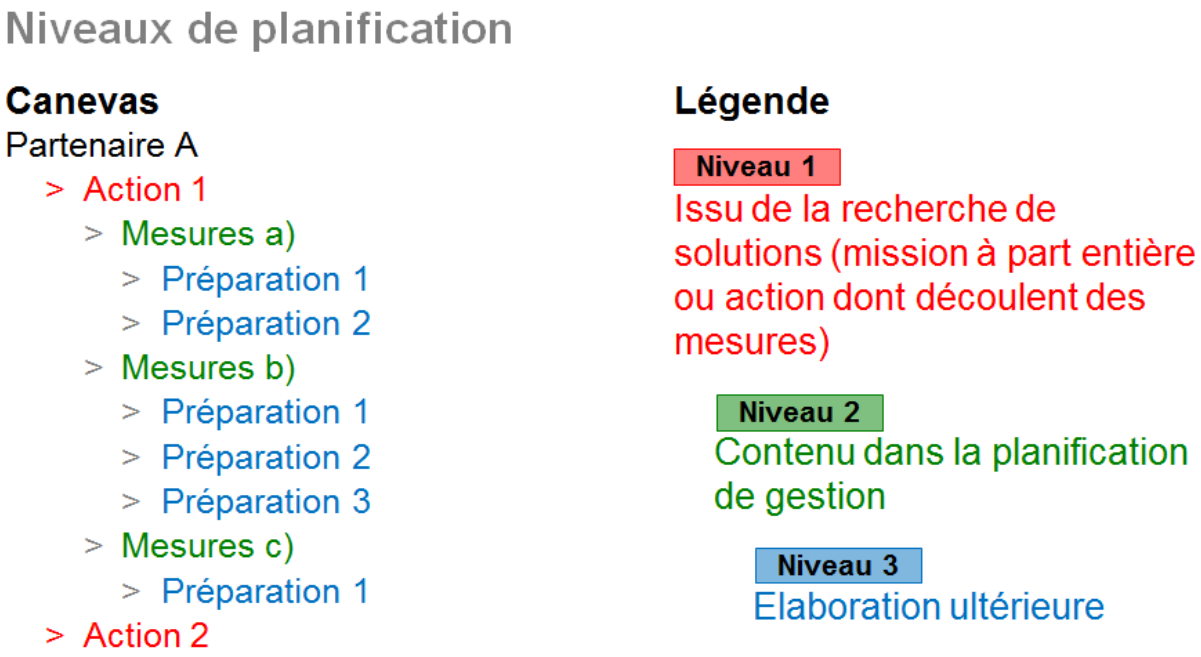

Figure 6: Niveaux de planification

Cette planification comprend ainsi les solutions possibles pour faire face à une telle situation, ainsi que les missions détaillées de chaque acteur. Ces acteurs sont responsables des mesures qu'ils veulent préparer, resp. tenir à disposition.

Les explications nécessaires à la compréhension et à l'utilisation du tableau de planification de gestion sont décrites à l'annexe 5.

4. Dispositions particulières

4.1. Collaboration

4.1.1. Interne au canton

Il est souhaitable que les entreprises annoncent également spontanément leur situation afin de consolider l'image de la situation cantonale. Ils jouent en effet un rôle important comme "lanceur d'alerte".

4.1.2. Externe au canton

4.1.2.1. Swiss Cyber Experts

Swiss Cyber Experts est composé d'un groupe d'experts hautement qualifiés de l'industrie des TIC, des milieux économiques, de l'administration et de l'académie. MELANI est chargé de coordonner leurs activités d'analyse, le tout dans l'anonymat du donneur d'ordre.

Swiss Cyber Experts permet aux entreprises privées et à l'administration de recourir à des experts hautement spécialisés dans le cas de cyber incidents graves. Le partenariat public-privé a pour but de fournir, tout en respectant la clause de confidentialité, un diagnostic rapide dans le cas de cyber incidents dont l'ampleur dépasserait les ressources des victimes, et crée ainsi les prémisses pour une solution efficace. Par contre, il ne contribue pas à la résolution de la panne, qui est l'affaire de l'entreprise.

Toute entreprise du canton peut faire appel à l'aide de ces spécialistes, en l'adressant à la protection de la population qui assurera le lien avec ce groupe.

4.1.2.2. Cyber-NDB

Le "Cyber-NDB"[13], dont fait partie MELANI, est la partie "cyber" du Service de renseignement de la Confédération. Il surveille et analyse la menace informatique et transmet les rapports de situation et autres information aux partenaires.

La protection de la population assure le lien avec le "Cyber-NDB".

Toute entreprise non-membre de MELANI peut, par l'intermédiaire de la protection de la population, annoncer toute panne, attaque ou défaillance à MELANI.

4.2. Renseignement

Le renseignement est l'affaire de tous. Chaque service organise le service de renseignement dans son service.

Les partenaires de l'OCC transmettent
> hors événement à la protection de la population
> dans l'événement à la CRens de l'OCC
spontanément ou sur demande, tous les renseignements, notamment quant à l'état de la situation et à leur engagement.

Par ailleurs, tout un chacun, notamment par le biais du CEA, peut signaler un événement.

---

[13] Nachrichtendienst des Bundes (Service de renseignement de la Confédération)

4.3. Information

4.3.1. Hors événement

En dehors d'un événement, la protection de la population assure l'information de ses partenaires, des organes de conduite, des exploitants d'infrastructures critiques et la population sur la situation, les menaces et les recommandations de comportement. A cet effet, elle se base sur les informations reçues de la Confédération, de ses partenaires et de son réseau d'entreprises et spécialistes TIC.

4.3.2. Dans l'événement

La conduite de l'information est assurée par la CInfo, conformément aux directives en vigueur au sein de l'OCC.

Dans la mesure du possible, les mesures de communication sont coordonnées avec les cantons voisins et la Confédération.

4.4. Communication

En cas de panne des systèmes d'information et de communication, des moyens alternatifs de communication, tels que recensés dans la planification de gestion (voir annexe 2), peuvent être utilisés/activés en fonction de leur opportunité, pertinence, disponibilité, durée de mise en service…. Ceux-ci, utilisables soit pour la communication interne ou la communication externe, peuvent être[14]:

> Affichage au pilier public
> Antennes mobiles (natel)
> Cloches des églises
> Emetteurs POLYCOM IDR
> Entreprises de courrier/transporteurs privés
> Estafettes ("Meldeläufer")
> Groupe des radio-amateurs[15]
> Haut-parleurs mobiles
> Hommes de liaison
> Hotline, yc. pour les formations d'intervention
> Largage de tracts par avion
> Pigeons-voyageurs
> Postes d'information
> Radio IPCC (IBBK-Radio)
> Répondeur automatique (pour les formations d'intervention et la population)
> Sirènes mobiles ou manuelles
> Tous-ménages

4.5. Confidentialité

Toute information obtenue hors et dans l'événement est strictement confidentielle et ne peut être transmise qu'aux personnes jugées nécessaires d'être mises au courant pour l'exécution de leurs tâches au sein de l'entreprise.

---

[14] Liste non exhaustive et sans ordre de priorité
[15] Faire attention à la confidentialité des données

4.6. Recommandations de comportement

Voir sous 4.3.1 "Hors événement" et sous www.fr.ch/catastrophe.

4.7. Mesures de contrainte[16]

L'OCC peut proposer au Conseil d'Etat notamment les mesures de contraintes ci-dessous:
> Obliger les entreprises à annoncer l'état de situation de leurs systèmes TIC
> Obliger les fournisseurs TIC de prendre:
  > Des mesures pour limiter l'ampleur de la panne
  > Des mesures coercitives vis-à-vis de la population
> Soumettre tous les médias à l'obligation d'annoncer[17]

En vertu de l'article 8 de la loi sur la protection de la population "*En cas d'événement, l'Etat et les communes prennent les mesures nécessaires pour faire face à la catastrophe ou pour maîtriser la situation d'urgence*", l'OCC pourra, par le biais du Conseil d'Etat, édicter dans l'événement toute autre mesure de contrainte.

Pour la population, l'OCC n'édictera que des recommandations de comportement.

4.8. Tests

Chaque acteur et chaque détenteur de systèmes d'information est tenu de tester régulièrement ses systèmes, ainsi que les systèmes et mesures redondants, alternatifs ou de secours,

4.9. Financement

4.9.1. Tests et mesures de préparation

Les frais liés à la prise de mesures de préparation sont à la charge de chacun.

4.9.2. A l'engagement

Le financement des engagements est assuré par l'Etat de Fribourg.

Le Conseil d'Etat peut entrer en matière pour une indemnisation des exploitants d'infrastructures critiques et des exploitants des réseaux TIC pour les éventuelles pertes financières dues aux mesures imposées.

5. Dispositions finales

Sur la base de la loi sur la protection de la population du 13 décembre 2007 (LProtPop), le présent plan d'engagement a été approuvé le 16 février 2017 en séance ordinaire de l'OCC. Le Conseil d'Etat en a pris acte le 25 avril 2017.

Le Service de la protection de la population et des affaires militaires (SPPAM) est chargé d'actualiser ce plan, en principe une fois par période législative pour autant que l'évolution de la situation ne l'ait pas exigé auparavant.

[16] Liste non exhaustive
[17] En référence à ICARO qui n'est une obligation que pour les radios et télévisions soumises à l'ORTV

Annexes

—

1. Matrice des responsabilités
2. Planification de gestion
3. Solutions - Inventaire
4. Actions – Description
5. Utilisation de planification de gestion

Distribution

—

Conseil d'Etat
Préfets
OCC
Spéc OCC dangers "Approvisionnement"
OCS
ORCOC
CEA
CASU144
SITel
EMF ABCN
MELANI
Infrastructures critiques (de criticité ≥3)

Impressum

Direction du projet
—
Organe cantonal de conduite OCC
Protection de la population

Rte des Arsenaux 16, Case postale 185, 1705 Fribourg

T +41 26 305 30 00, F +41 26 305 30 04
www.fr.ch/sppam

Renseignements
—
Service de la protection de la population et des affaires militaires SPPAM
Protection de la population

Rte des Arsenaux 16, Case postale 185, 1705 Fribourg

T +41 26 305 30 30, F +41 26 305 30 04
sppam_protpop@fr.ch, www.fr.ch/sppam

La version électronique du présent plan est téléchargeable sous:
www.fr.ch/catastrophe

Illustration de la page de titre
—
Photo: istockphoto.com

25 avril 2017