MEMOIRE DE FORMATION D'ADAPTATION A L'EMPLOI DE DIRECTEUR DEPARTEMENTAL ADJOINT

FAE 7
Session 2009

Les systèmes d'information des SDIS et les réseaux de l'Etat

« Quelles seront demain, les actions prioritaires à mettre en œuvre, visant à améliorer l'interopérabilité des systèmes d'information des différents acteurs concourant aux missions de sécurité civile et principalement, des SDIS ? »

Lieutenant-colonel Jean-Marc ANTONINI
Service départemental d'incendie et de secours des Landes

Directeur de mémoire : Monsieur Philippe DESCHAMPS
Adjoint au sous-directeur des sapeurs-pompiers et des acteurs du secours
Direction de la Sécurité Civile

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTERE DE L'INTERIEUR,
DE L'OUTRE-MER
ET DES COLLECTIVITES TERRITORIALES

REMERCIEMENTS

Je tiens à remercier en premier lieu Monsieur Robert CABE, Président du Conseil d'Administration du Service d'Incendie et de Secours des Landes, qui m'a permis de suivre cette formation.

Je remercie le Colonel Olivier BOURDIL, DDSIS 40, pour son soutien et ses encouragements.

Je remercie Monsieur Philippe DESCHAMPS qui a été un directeur de mémoire attentif, stimulant et un guide pour ce travail.

Merci à tous ceux qui, en me recevant ou en m'accordant un entretien téléphonique, ont contribué à ce mémoire :

Monsieur Thierry COURCET, chef du Groupement des Systèmes d'Information (GSI), SDIS 64 (Pyrénées Atlantiques) ; Lieutenant-colonel Pascal DEGUDE, chef du Groupement Informatique Transmissions Téléphonie (GITT) et Monsieur Christian DUCOURNEAU, GITT, SDIS 33 (Gironde) ; Lieutenant-colonel Dominique BONJOUR, chef du Groupement Opérations, SDIS 33 ; Monsieur Philippe ARNOULD, chef du Pôle des Systèmes d'Information et de Communication (PSIC) et Capitaine Stéphane POYAU, chef du Pôle des Méthodes Opérationnelles, groupement Opérations, SDIS 40 (Landes) ; Colonel Luc CORACK, chef de l'Etat-major de Zone (EMZ) Sud-Ouest et le Lieutenant-colonel Bruno DENAVE, EMZ Sud-Ouest ; Monsieur Pierre MACE, directeur du Groupement d'Intérêt Public Aménagement du Territoire et Gestion des Risques (GIP_ATGeRi) ; Colonel Hervé DOUTEZ, Monsieur Jean-Louis LENOC, Monsieur Laurent NEISIUS, Monsieur Bruno DOUSSINEAU, SDSPAS, DSC ; Lieutenant-colonel Fabien DIDIER, EMZ Sud ; Monsieur Serge RAVEZ, chef du Service Zonal des Systèmes d'Information et de Communication (SZSIC) de la zone Sud-Ouest et Monsieur Philippe BOUEY, SZSIC Sud-Ouest ; Lieutenant-colonel Didier FORTIN, chef du groupement de gendarmerie des Landes ; Monsieur Alain MANDINES, société SIS (ex-EDS) ; Lieutenant-colonel Patrick HEYRAUD, DDSIS 65 (Hautes-Pyrénées), Vice-président de la Fédération Nationale des Sapeurs-pompiers de France (FNSPF), président de la commission des Systèmes d'Information et de Communication (SIC) de la FNSPF, et le Lieutenant-colonel Hervé JACQUIN, DDA 65 ; Colonel Jean-Paul DESCELLIERES, DDSIS 33 et le Lieutenant-colonel Dominique MATHIEU, DDA 33 ; Capitaine Gilles DUBOS, membre de la commission SIC de la FNSPF, membre du Groupe de Travail 399 (GT 399), SDIS 33 ; Commandant Eric GIROUD, animateur de la commission SIC de la FNSPF, SDIS 88 (Vosges) ; Monsieur Bertrand GOMMER, responsable Grands Comptes, société Télédiffusion De France (TDF) ; Monsieur Jean de la RICHERIE et Madame Martine COUTURIER, société EADS ; Lieutenant-colonel Hervé PARIS, SDIS 01 (Ain) ; Colonel (ER) Jean-François SCHMAUCH ; Colonel Serge DELAIGUE, DDSIS 69 (Rhône) et lieutenant-colonel Lionel CHABERT, SDIS 69 ; Monsieur Marc PELLAS, Dirigeant de la société SYSTEL ; Monsieur Xavier PASCO, Fondation de la Recherche Stratégique (FRS) ; Colonel Gilles DAUTOIS, Madame Odile FAURE-JANDET et Monsieur Philippe VIOLET, Direction des Systèmes d'Information et de Communication (DSIC) ; Colonel Claude LORON, chef du bureau des Systèmes d'Information et Colonel Bertrand LOUARN, chef du bureau des Systèmes de Communication, Direction Générale de la Gendarmerie Nationale (DGGN) ; Docteur Eric LECARPENTIER, SAMU de France, SAMU 94 (Val de Marne) ; Commissaire Dimitri KALININE, chef de la Division des programmes opérationnels, Service des Technologies et des Systèmes d'Information (STSI), Direction Générale de la Police Nationale (DGPN) ; Monsieur Pierre-Louis GAVHAM, Directeur des Systèmes d'Information (DSI) du Conseil Général des Landes ; Monsieur Jean ROUX, Directeur territorial adjoint, ERDF-Gironde (33).

Merci à tous ceux qui m'ont prodigué conseils et soutien et qui ont pris le temps de répondre à mes questions par courriel :

Lieutenant-colonel Georges RINGOTTE, directeur opérationnel, SDIS 84 (Vaucluse) ; Commandant Xavier PERGAUD, chef du groupement opérations, SDIS 47 (Lot et Garonne) ; Lieutenant-colonel Michel CARRASSET, chef du groupement sud-ouest, SDIS 33, Lieutenant-colonel Bertrand DOMENEGHETTI, chef du groupement de Libourne, SDIS 33 (Gironde) ; Colonel Henri BENEDETTINI, DDSIS 11 (Aude) ; Colonel François MAURER (ER), ancien président du CTIF ; Lieutenant-colonel Christophe MIGNOT, Ecole Nationale Supérieure d'Officiers de Sapeurs Pompiers (ENSOSP), secrétaire général du CTIF ; Commandant Claire KOWALEWSKY, Mission des Relations Internationales (MRI), DSC ; Lieutenant-colonel Frédérique FICHAUX-CASANOVA, EMZ Sud-Ouest ; Lieutenant-colonel François GROS, directeur opérationnel et technique, SDIS 64 ; Commandant Bruno MAESTRACCI, DDA SDIS 2A (Corse du sud) ; Alphonse PHILIPPE, GT 399, INFOCERT ; "Fire Safety and rescue" Directorate General, Bulgaria ; Pekka TULOKAS, Department for Rescue Services, Ministry of the Interior, Finland ; Kaspars KIESNERS, IT&T nodalas, Latvia ; ROUMPOU Katerina, Hellenic Fire Service, Information Technology and Communication Department ; Dennis DAVIS, Chairman, Federation of British Fire Organisations ; Frédéric JORAND, Service Assurance Manager POLYCOM, Département fédéral de la défense, de la protection de la population et des sports (DDPS), Office fédéral de la protection de la population (OFPP) ; Russell E. SANDERS, President United States Delegation CTIF ; Dieter NUESSLER, president of the FEU ; Commandant Olivier LOUSTAU, chef du pôle Prévision-Planification, groupement Opérations, Commandant Jean-Yves PEREZ, chef du groupement de Mont-de-Marsan, Monsieur Jean-François MESPLEDE, PSIC, et Mesdames Delphine CHUSSEAU, Odile DESTENAVE, Cathy LAFOURCADE, SDIS 40.

AVERTISSEMENT

Les opinions émises dans ce document n'engagent que leur auteur. Elles ne constituent en aucune manière une position officielle du ministère de l'Intérieur, de l'Outre-Mer et des Collectivités Territoriales.

« Pour être plus il faut s'unir, pour s'unir il faut partager, pour partager il faut avoir une vision » Pierre Teilhard de Chardin.

SOMMAIRE

RESUME

Les Nouvelles Technologies de l'Information et de la Communication (NTIC) sont au confluent de trois technologies : les technologies des télécommunications, celles de l'Internet et les technologies informatiques. Leur formidable développement et leur importance croissante dans les sphères professionnelle et privée révolutionnent l'organisation de nos sociétés post-industrielles qui basculent dans un nouveau schéma sociétal : la société de l'information en réseau.
L'utilisation des systèmes d'information et de communication (SIC) interconnectés sur les réseaux permet d'atteindre un niveau de maîtrise de l'information à la hauteur des nouvelles exigences de protection des populations.

En effet, l'impact national voire supra national des nouveaux risques et menaces (accidents technologiques, catastrophes naturelles, pandémies, attaques terroristes) a une conséquence directe sur l'ensemble des services de secours et de sécurité. Ces services ne peuvent plus continuer à agir séparément, selon leur propre logique « verticale » mais doivent développer leur interopérabilité.
Partout en Europe, des réseaux nationaux de radiocommunication numériques sont déployés, partagés par les « blue light services » (forces de sécurité intérieure). En France, c'est l'Infrastructure Nationale Partagée des Transmissions (INPT) qui progressivement relie policiers, pompiers, services d'aide médicale urgente, gendarmes…

L'objectif est de faire travailler ensemble les différents acteurs. Le cloisonnement de leurs organisations doit être dépassé sur la base d'une organisation de sécurité civile fonctionnant en réseau.

Ce mémoire présente les concepts de base des réseaux et de l'interopérabilité. Il fait un état des lieux des acteurs, notamment sapeurs-pompiers, et des réseaux de l'Etat. Il examine les réseaux nationaux de radiocommunication numériques partagés de cinq pays européens (Angleterre, Belgique, Suisse, Espagne et Finlande).

Autour de la problématique de la *mise en réseau des différents acteurs concourant aux missions de sécurité civile*, un diagnostic est établi. Il identifie les opportunités à saisir, les faiblesses à combler, les compétences à développer et les forces sur lesquelles peuvent s'appuyer les différents services pour interconnecter leurs systèmes d'information et commencer à bâtir le réseau de la sécurité civile.

Présentées sous la forme d'un plan stratégique 2010-2020, vingt-six recommandations sont émises à partir de quatre orientations : Mettre en place une gouvernance des SIC ; Réaliser un référentiel d'interopérabilité ; Maîtriser les NTIC ; Développer une culture de l'interopérabilité.
Du fait de leur fort impact et de leur facilité de mises en œuvre, six recommandations sont identifiées comme pouvant être mises en œuvre immédiatement.

Enfin, ce mémoire se termine par une interrogation : dans la nouvelle architecture de sécurité nationale voulue par le livre blanc de la Défense et de la Sécurité nationale, quelle sera la place de la sécurité civile ?

SUMMARY

The new Information Technology combines three different technologies-telecommunications, Internet and computer systems. Their tremendous development and their growing importance in professional and private spheres have revolutionized the organisation of our post-industrial societies which are now following a new societal development plan: the society of information network.
The use of information systems interconnected on networks makes it possible to reach a level of control over the information in keeping with today's demands to protect populations.

Indeed the new risks and threats (technological accidents, natural disasters, pandemics, terrorist attacks) having national or even supra national impact, also directly affect the rescue and emergency services altogether. These services can no longer work separately but have to develop their interoperability.
Everywhere in Europe, national digital radio communication networks are deployed and shared by the blue light services. In France the INPT (Shared National Infrastructure of Transmission) gradually links together the police, the fire-fighters, the paramedics, the health services, the French "gendarmerie"…

The objective is to have the different protagonists to work together. The barriers between their organisations must be broken down and a new organisation of the civil security based on networks must be built up.

This study presents the basic concepts on networks and interoperability. It draws up an inventory of the protagonists, namely the fire-fighters, and the State networks. It examines the shared national digital radio communication networks in five European countries (England, Belgium, Switzerland, Spain and Finland).

A diagnosis is made from the inherent problem of this research -*networking the different services responsible for the protection and rescue of the population*. It identifies the opportunities to be grasped, the weaknesses to be overcome, the skills to be developed and the forces on which the different services can rely so as to interconnect their information systems and therefore start building up the network of the civil security.

In a strategic plan for 2010-2020, twenty-six recommendations are presented according to four different directions: implement a governance of the information systems; create a system of reference in interoperability; control the new I.T; develop common values on interoperability.
Considering their massive impacts and their easy implementations, six recommendations can be immediately set up.

Lastly, this study ends up with a question: what role will the civil security have in the new organisation of the national security, which is carried out in accordance with "le livre blanc de la Défense et de la Sécurité nationale"?

INTRODUCTION

La révolution des nouvelles technologies de l'information et de la communication engendre une nouvelle société : la « société de l'information[1] » ou « société en réseaux[2] ».
Marqué par le mouvement et l'interdépendance, le monde nouveau qui se dessine s'accompagne de nouveaux risques et menaces (attentats terroristes, catastrophes climatiques, pandémies) qui révèlent la vulnérabilité des territoires et des populations.
Les attentats terroristes de New York, de Madrid, de Londres, ont mis en évidence le manque de coordination entre les différents services d'intervention (pompiers, police, santé, armée, …).

Face à ces nouveaux risques et menaces d'ampleur, l'interopérabilité des différents services est devenue une nécessité.

Le déploiement d'infrastructures de radiocommunication numérique et la généralisation des systèmes d'information dans les organisations, permettent de réaliser cette interopérabilité.

En France, l'Etat est le garant de la cohérence de la sécurité civile au plan national. Il lui appartient donc, de réfléchir au « réseau de sécurité civile » qui doit se mettre en place.

Mais comment s'y prendre pour développer l'interopérabilité entre autant d'acteurs divers ? Et, à l'horizon de 10 ans, comment faire travailler ensemble les différents acteurs concourant aux missions de sécurité civile ? Comment les mettre en réseau ?

Après avoir abordé les notions de *réseaux*, de *systèmes d'information* et d'*interfaces*, nous définirons l'interopérabilité et ses enjeux. Nous ferons un état des lieux des acteurs, notamment des services départementaux d'incendie et de secours (SDIS), avant d'examiner la situation des réseaux de l'Etat et de quelques pays européens.

Sur la base des fondements trouvés dans les orientations de la politique de sécurité civile, nous établirons un diagnostic des opportunités à saisir, des faiblesses à combler, des actions à entreprendre et des savoir-faire à utiliser pour construire le réseau des acteurs concourant à la sécurité civile.

Un plan d'action stratégique (2010-2020) présentera les orientations et les recommandations issues de cette étude.

« *A l'évidence, la sécurité civile ne doit pas s'enfermer dans le cadre traditionnel de l'Etat régalien. Sa modernisation s'inscrit dans la définition renouvelée d'un Etat apte à promouvoir et fédérer les compétences et capacités de toute la société civile, et tirant son autorité du succès des coopérations qu'il organise*.[3] »

[1] Information : élément de connaissance susceptible d'être représenté à l'aide de conventions pour être conservé, traité ou communiqué, *in futura-sciences.com*
[2] Castells M. 1998, *La société en réseaux*, Fayard.
[3] Extrait de l'intervention de M. Nicolas SARKOZY, ministre d'Etat, ministre de l'intérieur et de l'aménagement du territoire à l'occasion de l'installation du Conseil National de la Sécurité Civile – Hôtel de Beauvau – vendredi 2 décembre 2005.

1 SOCIETE EN RESEAUX ET RESEAUX DE SECURITE CIVILE

1.1 Réseaux et interopérabilité

1.1.1 Un monde virtuel bien réel

Du télégraphe au NTIC

Dans l'histoire humaine, chaque avancée technologique dans le domaine des communications a provoqué une rupture. Ainsi, le télégraphe optique de Claude Chappe (1763-1805) a permis à Napoléon de diriger son empire et de commander son armée.
Avec le signal électrique, le télégraphe est devenu planétaire. Puis le téléphone et la radiocommunication sont apparus.
A partir des années soixante, l'avènement de l'informatique révolutionne le traitement et la circulation de l'information. Avec la numérisation du signal électrique analogique, les réseaux informatiques[4] se confondent avec ceux des communications.
De nos jours, les NTIC[5] (nouvelles technologies de l'information et de la communication) associent les technologies des télécommunications à celles de l'informatique et d'Internet (protocole IP[6]). Ces technologies concilient puissance de traitement et miniaturisation des composants et ne cessent d'évoluer.

Sur les réseaux de transmissions circulent toujours plus d'informations dans toujours plus de lieux.

Les réseaux : les liens structurants

Le réseau structure logiquement une organisation dans l'espace en reliant hiérarchiquement les systèmes de l'organisation.
Le réseau filaire téléphonique, très bien maillé, a permis le déploiement rapide de l'Internet[7] au bénéfice des entreprises comme des particuliers.
La fibre optique qui permet d'atteindre de très hauts débits et les technologies « sans fil » se développent (Wi-max, faisceaux).
Les besoins en téléphonie mobile ont nécessité l'installation d'un réseau d'antennes GSM[8] sur des points hauts existants ou créés pour l'occasion. Aujourd'hui, ce réseau couvre largement le territoire et les débits offerts par la 3ème génération (3G) permettent la transmission d'images vidéo.
Depuis l'espace, les satellites offrent une solution alternative et complémentaire aux réseaux terrestres.

La mise en réseau des systèmes informatiques crée des systèmes globaux de gestion des entreprises et des organisations basés sur l'échange et le traitement de l'information en temps quasi-réel : les systèmes d'information (SI) ou systèmes d'information et de communication (SIC).

---

[4] Un réseau informatique est un ensemble d'équipements reliés entre eux pour échanger des informations (*encyclopédie libre Wikipédia*).
[5] Ou TIC (Technologie de l'Information et des Communications), IT (Information Technology).
[6] Internet Protocol.
[7] Internet : le réseau des réseaux interconnectés à l'échelle de la planète. Selon que le réseau (privé) est interne ou externe à l'organisation, on parlera de « Intranet » ou de « Extranet ».
[8] Global System for Mobile communications.

Le SI : incarnation d'une stratégie et d'un modèle d'organisation

Il existe de nombreuses définitions du SI.

Le SI peut s'entendre comme un « *ensemble organisé des matériels, personnes et équipements permettant de stocker, transmettre et traiter de l'information* » ou encore comme un « *ensemble d'applications informatiques supportant les activités des individus dans les organisations*[9] ».
L'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques définit le SI comme « *tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives* ».

Il y a derrière ce terme, une notion d'organisation. Le SI est aligné sur la stratégie de l'entreprise[10] ; il en est l'incarnation.

Les étapes de conception du SI de l'entreprise peuvent être résumées comme suit :

- 1-Définition de la stratégie,
- 2-Analyse du fonctionnement des services et des processus (tâches, activités),
- 3-Optimisation des processus et réorganisation des services,
- 4-Conception (architecture, urbanisation) du SI autour de cette réorganisation,
- 5-Après une phase de fonctionnement, correction du SI (réalignement du SI) sur la stratégie.

Le SI permet un meilleur partage des informations et de la connaissance entre les différentes composantes de l'organisation. Il offre l'opportunité de prises de décisions rapides sur la base d'indicateurs précis et mesurés.
Le but au final est d'obtenir des gains significatifs de productivité/efficacité.
Les entreprises du secteur bancaire et industriel, celles des services commerciaux, c'est-à-dire celles qui ont besoin de toujours plus de puissance de calcul et de rapidité dans les échanges ont été parmi les premières à remodeler leur organisation autour des SIC.

La communication entre les systèmes, parfois différents, et leurs échanges et interactions sont rendus possibles par l'utilisation d'interfaces.

L'interface : « l'arme qui unit les armes[11] *»*

Une interface est un point à la frontière entre deux éléments, par lequel ont lieu des échanges et des interactions[12].
L'interface homme-machine (IHM) et l'interface utilisateur donnent accès aux fonctions du programme par le biais d'un clavier, d'une souris ou d'un écran tactile tout en les représentant d'une manière graphique.
L'interface de programmation (API[13]) permet des échanges entre plusieurs logiciels. Elle consiste à la mise à disposition, sous format libre ou propriétaire, d'un ensemble de fonctions qui ainsi peuvent être mises en œuvre par des programmes informatiques sous différents systèmes d'exploitation.

[9] Définition donnée par J. Akoka, professeur au CNAM et à l'INT (Institut National des Télécommunications).
[10] Le système d'information transverse, 2008 :16.
[11] Adage militaire cité par M. Philippe Deschamps, directeur de mémoire.
[12] Dictionnaire Larousse, Editions 2006.
[13] Application Programming Interface.

Une interface communément utilisée peut devenir une norme édictée par un ou des organismes de régulation, souvent internationaux. Ce type d'interface permet de relier des systèmes de constructeurs différents.

Ils constituent des réseaux de systèmes dits interopérables.

1.1.2 L'interopérabilité

Nous distinguerons deux types d'interopérabilité :

- une interopérabilité technique au niveau des systèmes matériels,
- une interopérabilité des doctrines.

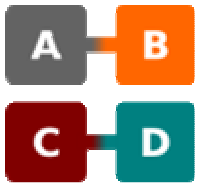
Puis nous évoquerons les enjeux de l'interopérabilité.

L'interopérabilité technique

Dans le domaine informatique, l'interopérabilité est « *la capacité que possède un produit ou un système, dont les interfaces sont intégralement connues, à fonctionner avec d'autres produits ou systèmes existants ou futurs et ce sans restriction d'accès ou de mise en œuvre*[14] ».

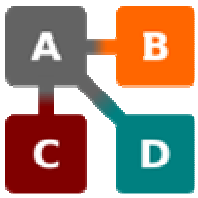
On distingue trois degrés d'opérabilité[15].

- La **compatibilité**



La compatibilité est la possibilité pour deux systèmes de types différents de communiquer ensemble.

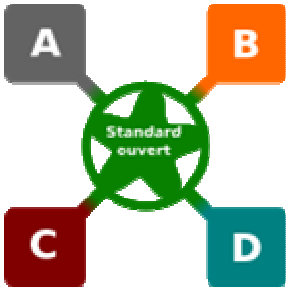
- Le **standard de fait**



Lorsqu'un acteur devient dominant dans un domaine, les autres acteurs font en sorte d'être compatibles avec lui.
Avantage : tous les systèmes peuvent à peu près communiquer ensemble.
Inconvénient : l'acteur dominant contrôle d'une certaine manière cette possibilité.

[14] Définition issue des travaux du groupe de travail sur l'interopérabilité de l'Association Francophone des Utilisateurs de Logiciels Libres, AFUL.
[15] Schémas et commentaires sur les degrés d'opérabilité sont extraits des travaux du groupe de travail sur l'interopérabilité de l'AFUL.

- L'**interopérabilité**



L'interopérabilité est la possibilité pour différents systèmes de communiquer entre eux sans dépendre d'un acteur particulier. Elle repose sur la présence d'un standard ouvert.

Seule la connaissance exhaustive des interfaces d'un produit ou d'un système permet d'en garantir l'interopérabilité.

La téléphonie est un exemple de systèmes interopérables. La standardisation des interfaces garantit le bon fonctionnement de tout type d'appareils et de matériels qui respectent les normes en la matière[16].

Un autre exemple de systèmes interopérables est Internet. L'adoption d'un protocole unique (TCP/IP[17]), hébergé dans chaque ordinateur, permet l'utilisation de tout réseau existant. La page web est un standard unique facilitant l'apprentissage par tout utilisateur. Des instances de régulation et de coordination assurent son évolution et veillent à l'adoption de règles communes.

De ces exemples, il ressort que l'interopérabilité des systèmes nécessitent de remplir 3 conditions :

- un protocole de communication unique ;
- des interfaces standardisées ;
- des organismes de régulation.

Les organisations qui recherchent l'interopérabilité de leurs systèmes doivent apporter des réponses à des questions essentielles liées au partage de l'information.

- Pourquoi voulons-nous échanger ?
- Avec qui voulons-nous échanger ?
- Quelles informations voulons-nous échanger ?
- Selon quelles règles et procédures ?

L'interopérabilité technique ne suffit donc pas.

En effet, l'interopérabilité possède un sens plus large qui vise à faire travailler ensemble, comme un seul corps, des organisations différentes pour atteindre un objectif commun.

[16] Les normes de téléphonie sont gérées par l'Union Internationale des Télécommunications (UIT).
[17] Transmission Control Protocol/Internet Protocol

L'interopérabilité des doctrines

La notion d'interopérabilité apparaît au lendemain de la seconde guerre mondiale. Les forces de l'alliance atlantique (OTAN[18]) doivent pouvoir opérer de concert entre elles et sous l'autorité des commandements centraux. Le besoin d'interopérabilité découle de cette obligation. Des documents de standardisation sont établis couvrant des domaines allant de la doctrine à la technique en passant par les équipements et les communications : les STANAG (STANdardization AGreements).

Plus récemment, le livre blanc de la Défense et de la Sécurité nationale[19] définit l'interopérabilité comme la « *capacité de plusieurs systèmes, unités ou organismes à opérer ensemble grâce à la compatibilité de leurs organisations, doctrines, procédures, équipements et relations respectives* ».

Les enjeux de l'interopérabilité

L'interopérabilité est cruciale car aujourd'hui, dans tous les secteurs d'activité, des SI gèrent des données, et pilotent les outils de gestion et de contrôle.

- Un enjeu stratégique de puissance et de domination.

Vers la fin des années 90, aux Etats-Unis, dans le domaine militaire, l'évolution des TIC donne naissance à la doctrine du « Network-Centric Warfare[20] » (NCW). Cette doctrine transforme l'art de la guerre par l'utilisation des réseaux. Il s'agit de connecter l'ensemble des ressources, des services, des données, des programmes pour permettre à n'importe quel personnel de disposer des informations utiles en fonction de sa mission.
Ce concept est passé dans le domaine civil. Les entreprises américaines, fortes de leur avance technologique, édictent leurs normes et imposent leurs standards dans le cadre d'une stratégie économique visant à dominer le marché mondial[21].
Dans le domaine de l'informatique, nous assistons à une lutte entre des formats dits « propriétaires » et des formats dits « ouverts » (ou « open source »)[22].
Pour rattraper son retard technologique et construire son indépendance géopolitique, L'Union Européenne investit dans la recherche et le développement des NTIC avec pour enjeu, la maîtrise de l'interopérabilité des systèmes sur la base de standards ouverts.

- Un enjeu opérationnel de maîtrise de l'information.

Pour le livre blanc de la Défense et de la Sécurité nationale, « *l'interopérabilité des réseaux d'information, qui optimise la circulation de l'information* », est un des quatre piliers de la maîtrise de l'information[23]. Elle garantit un commandement efficace en opérations en apportant au décideur l'information utile, en temps et en qualité, dont il a besoin. Elle apporte plus de sécurité aux intervenants sur le terrain.

---

[18] Organisation du Traité de l'Atlantique Nord.
[19] Livre blanc de la Défense et de la Sécurité nationale, Juin 2008, glossaire.
[20] Opération réseau-centré.
[21] Paul Romer est l'un des principaux théoriciens américains de la croissance économique, qu'il voit tirée par l'innovation technologique. Celle-ci concerne tous les aspects de la société (changement de paradigme).
[22] Voir à ce sujet les débats autour de l'élaboration du référentiel général d'interopérabilité (RGI) relatif aux formats des données électroniques dans l'administration.
[23] La stratégie de sécurité nationale est guidée par 3 principes : Anticipation/Réactivité, Résilience, Capacité de montée en puissance. Elle repose sur la combinaison de 5 grandes fonctions stratégiques : Connaissance/Anticipation, Prévention, Dissuasion, Protection, Intervention. La maîtrise de l'information est un des 5 domaines de la fonction stratégique Connaissance/Anticipation.

1.2 Acteurs et réseaux

1.2.1 Les acteurs concourant aux missions de sécurité civile

Une diversité d'acteurs

La loi de modernisation de la sécurité civile[24] dans son article 2 définit clairement les acteurs de la sécurité civile en distinguant ceux qui en assurent principalement les missions de ceux qui y concourent.
Les acteurs principaux sont :

- les sapeurs-pompiers professionnels et volontaires des services d'incendie et de secours ;
- les personnels des services de l'Etat et les militaires des unités qui en sont investis à titre permanent.

Les acteurs qui concourent aux missions de sécurité civile sont :

- les militaires des armées et de la gendarmerie nationale ;
- les personnels de la police nationale ;
- les agents de l'Etat, des collectivités territoriales et des établissements et organismes publics ou privés appelés à exercer des missions se rapportant à la protection des populations ou au maintien de la continuité de la vie nationale ;
- les membres des associations ayant la sécurité civile dans leur objet social ;
- les réservistes de la sécurité civile.

Enfin, la loi dans son article 4, implique chaque citoyen : « *toute personne concourt par son comportement à la sécurité civile*[25] ».

La sécurité civile se caractérise donc par la diversité de ses acteurs. Cette diversité trouve sa justification dans la pluralité des risques (courants ou particuliers, nouveaux risques et menaces) et leurs différents niveaux (local, régional, national).

Une coproduction Etat/Collectivités Locales

L'Etat est le garant de la cohérence de la sécurité civile au plan national[26] et les sapeurs pompiers sont au cœur du dispositif. Leurs établissements publics, les SDIS, exercent les missions de sécurité civile à l'échelle du territoire du département, impliquant de fait les collectivités territoriales du département[27].
D'autre part, la notion de résilience[28] introduite par le livre blanc de la Défense et de la Sécurité nationale, donne aux collectivités territoriales un rôle complémentaire à celui de l'Etat dans l'organisation des pouvoirs publics.

Dans la logique de la décentralisation, nous pouvons dire que la sécurité civile est une coproduction Etat/Collectivités Locales.

---

[24] Loi n° 2004-811 du 13 août 2004 de modernisation de la sécurité civile
[25] « *La sécurité civile est l'affaire de tous* ». Ce principe est une réaffirmation du principe républicain dont nous pouvons retrouver l'origine dans le décret révolutionnaire du 16-24 août 1790. Ce texte qui donne au maire les pouvoirs de police en mobilisant les ressources des citoyens constitue l'acte de naissance de la sécurité civile moderne. De cet engagement civique sont issus les sapeurs pompiers. Cet engagement civique perdure encore de nos jours à travers l'engagement des sapeurs pompiers volontaires.
[26] Article 1, loi n° 2004-811 du 13 août 2004 de modernisation de la sécurité civile.
[27] Le SDIS est un établissement public départemental, financé par les communes et le Conseil Général et administré par un conseil d'élus représentant les communes et le département, présidé par le Président du Conseil Général ou un élu désigné par lui.
[28] « *La résilience se définit comme la volonté et la capacité d'un pays, de la société et des pouvoirs publics à résister aux conséquences d'une agression ou d'une catastrophe majeures, puis à rétablir rapidement leur capacité de fonctionner normalement, ou à tout le moins dans un mode socialement acceptable. Elle concerne non seulement les pouvoirs publics, mais encore les acteurs économiques et la société civile tout entière* » (Livre blanc de la Défense et de la Sécurité nationale, 2008 :64).

Les rôles principaux

Les principaux acteurs sont ceux qui jouent un rôle opérationnel majeur sur le terrain. Les anglo-saxons les regroupent sous le terme des « blue light services »[29] soit, pour la France : les pompiers, la police, la gendarmerie et les SAMU[30].

Sur quels réseaux (de l'Etat) ces services s'appuient-ils ?

1.2.2 Les réseaux de l'Etat

Ils peuvent être classés en trois catégories :

- les réseaux de messagerie et de téléphonie (serveur web), de partage d'informations (intranet) et de téléphonie, reposant généralement sur les infrastructures des opérateurs de téléphonie et fournisseurs d'accès Internet (FAI) ;
- le réseau national d'alerte (RNA) ;
- les réseaux radioélectriques analogiques remplacés progressivement par la technologie numérique (TETRAPOL).

Les réseaux de messagerie et de téléphonie

- Le RGT (Réseau Général de Transmissions), intranet sécurisé, qui comprend :
  - la messagerie opérationnelle chiffrée RESCOM ;
  - le téléphone « durci » RIMBAUD pour la communication interministérielle sécurisée entre hautes autorités ;
  - le portail ORSEC[31] (ex-SYNERGI), intranet utilisé, entre autres, par les CODIS pour la remontée des événements opérationnels vers les préfectures, le COZ et le COGIC[32].
- Les réseaux du gouvernement qui équiperont prochainement les préfectures :
  - ISIS (Intranet Sécurisé Interministériel pour la Synergie gouvernementale), un intranet sur un réseau indépendant à base de fibres optiques. Il est à noter que la migration du portail ORSEC sur ISIS est à l'étude ;
  - le système MAGDA (Messagerie Autonome Gouvernemental de Défense et d'Autorité), messagerie électronique sécurisée reliée à ISIS.
- SAPHIR, la messagerie opérationnelle de la gendarmerie, intranet sécurisé, qui est l'équivalent du RGT.

Le réseau national d'alerte (RNA)

Ce réseau à base de sirènes déclenchées par les préfectures dont l'origine remonte à la guerre froide est devenu obsolète. Il va progressivement être remplacé par le Système d'Alerte et d'Information des Populations (SIAP), expérimenté avec succès dans la Zone de Défense Sud-Est avec le SDIS 01 (Ain).
Le SIAP utilise les possibilités offertes par les technologies de radiocommunication numériques et pourra s'interconnecter avec les autres dispositifs d'informations des populations (panneaux électroniques d'informations des autoroutes, des villes, etc.). Le déclenchement des sirènes pourra s'effectuer à partir des systèmes d'aide à la décision des centres opérationnels des SDIS (CODIS).

---

[29] Littéralement « les services des gyrophares bleus »
[30] Service d'Aide Médicale Urgente.
[31] ORganisation des SECours.
[32] Centre Opérationnel Zonal et Centre Opérationnel de Gestion Interministérielle des Crises.

Les réseaux radioélectriques :

- RUBIS, le réseau radio de la gendarmerie nationale. Mis en place en 1993, c'est le premier réseau radio numérique utilisée par une force de sécurité dans le monde. L'infrastructure déployée à base de faisceaux couvre l'ensemble du territoire ;
- ACROPOL[33], le réseau radio de la police nationale. Son infrastructure à base de faisceaux et de lignes spécialisées couvre 65% du territoire, essentiellement les agglomérations ;
- ANTARES[34], le réseau des services d'incendie et de secours, des moyens d'Etat de la Sécurité Civile et des SAMU. C'est une extension du réseau ACROPOL. Le programme d'extension de l'infrastructure piloté par la DSC[35] vise à compléter la couverture du territoire pour réaliser une Infrastructure Nationale Partagée des Transmissions (INPT) ;
- CORAIL NG, le réseau de la gendarmerie mobile intégrée à l'INPT.

La technologie numérique chiffrée TETRAPOL, déjà utilisée par la police et la gendarmerie, remplace progressivement les anciens réseaux analogiques des moyens d'Etat de la Sécurité Civile, des sapeurs pompiers et des SAMU.

L'INPT : première étape de l'interopérabilité

« *L'infrastructure réalisée par l'interconnexion des réseaux de base départementaux constitue une infrastructure nationale partageable des transmissions (INPT)*[36] ».

L'INPT est le réseau national français de radiocommunication numérique dédié aux forces de secours et de sécurité. Il est basé sur la mutualisation des infrastructures et le partage des ressources.
L'infrastructure du réseau déployé par l'Etat au profit de la police nationale constitue l'infrastructure de base de l'INPT. Cette infrastructure de 1100 relais a été portée à 1450 relais pour une couverture de 95% de l'ensemble du territoire.
A terme, l'INPT sera exploitée par plus de 100 000 terminaux.

Ses objectifs fonctionnels sont :

- l'interopérabilité tous services ;
- une mobilité nationale ;
- une extension des services « voix » (appel individuel, interopérabilité tactique) ;
- des applications fondamentales « données » (status, géolocalisation, appel de détresse, …) ;
- des développements d'applications « métiers » (standardisation des interfaces ouvertes, AFNOR[37]) ;
- des mutualisations d'équipements et d'applications ;
- une culture commune d'exploitation opérationnelle des transmissions (doctrine d'emploi, applications d'échanges de données, …).

Les services utilisateurs de l'INPT - autres que la police nationale - sont les moyens nationaux de la sécurité civile, les services d'incendie et de secours, la brigade des

[33] Automatisation des Communications Radio Opérationnelles de la Police.
[34] Adaptation Nationale des Transmissions Aux Risques Et aux Secours.
[35] Direction de programme ANTARES, SDSPAS.
[36] Article 5 du décret n°2006-106 du 3 février 2006 relatif à l'interopérabilité des réseaux de communication radioélectriques des services publics qui concourent aux missions de sécurité civile.
[37] Agence Française de NORmalisation.

sapeurs-pompiers de Paris (BSPP), le bataillon de marins-pompiers de Marseille (BMPM), la gendarmerie nationale et les services d'aide médicale urgente[38] (SAMU).
L'infrastructure des services utilisateurs intègre l'INPT soit sous réserve d'une vérification d'aptitude technique[39], soit au fur et à mesure de leur renouvellement après une mise en conformité[40].
Le Ministre de l'Intérieur est le coordonnateur national de l'INPT et le garant de sa cohérence d'ensemble. Un comité de pilotage propose sur la base d'indicateurs fournis par le coordonnateur national, les orientations relatives au déploiement des réseaux, à leur fonctionnement et à leurs évolutions[41]. La composition de ce comité a été fixée par un arrêté en date du 24 février 2009[42].

Le réseau ANTARES sera ouvert sur l'ensemble du territoire métropolitain dès 2010.
17 SDIS ont totalement migré sur ce réseau. 75 SDIS sont en cours de migration. Cette phase doit s'achever en 2015[43]. Le parc des postes radio des SDIS et de la BSPP a basculé à plus de 30% des anciens réseaux analogiques au réseau ANTARES.

La Direction de l'hospitalisation et de l'organisation des soins (DHOS) du ministère de la Santé a diffusé un guide relatif au mode opératoire pour la migration des SAMU sur ANTARES. Cette migration doit se faire de manière synchronisée avec celle des SDIS[44].
Les moyens nationaux de la sécurité civile (service déminage, UIISC, ESOL[45]) sont dotés de postes ANTARES qui leur permettent d'être interopérables sur l'ensemble du territoire. Les moyens aériens sont en cours d'équipement.

L'intégration à l'INPT du réseau RUBIS de la gendarmerie est prévue en 2020. En attendant, les centres opérationnels de la gendarmerie s'équipent de postes ANTARES pour assurer une interopérabilité minimale.

En regroupant à terme l'ensemble des acteurs des secours, l'INPT apparaît comme le premier pas vers l'objectif d'interopérabilité affichée par l'article 9 de la loi de modernisation de la sécurité civile[46].

Observations sur L'INPT[47]

- Les réseaux TETRAPOL RUBIS et ACROPOL/ANTARES n'utilisent pas la même bande de fréquence (80MHz pour RUBIS, 400MHz pour ACROPOL/ANTARES). La gendarmerie affiche sa volonté de rester dans la bande des 80MHz et souhaite mixer les deux réseaux.
- L'INPT est basé sur une architecture départementale RB (réseau de base). L'interconnexion RB est possible mais consomme beaucoup de ressources.
- En raison des investissements importants à réaliser (il faut changer les terminaux et adapter ou renouveler les équipements des CTA/CODIS[48]), la migration des SDIS s'effectue sur plusieurs exercices budgétaires. Pendant cette phase transitoire, vont coexister des équipements de technologies différentes.

---

[38] Articles 2 et 6 du décret n°2006-106.
[39] Article 7 du décret n°2006-106.
[40] Article 3 du décret n°2006-106.
[41] Article 11 du décret n°2006-106.
[42] Arrêté du 24 février 2009 fixant la composition du comité de pilotage de l'infrastructure nationale partageable des transmissions.
[43] Données INFOSDIS 2008.
[44] Circulaire DHOS/O1/F2 n° 2009-228 du 22 juillet 2009.
[45] Unité d'Instruction et d'Intervention de la Sécurité Civile. Etablissement de Soutien Logistique.
[46] « *Un décret fixe les règles et normes techniques permettant d'assurer l'interopérabilité des réseaux de communication radioélectriques et des systèmes d'information des services publics qui concourent aux missions de sécurité civile.* ».
[47] Recueillies lors des différents entretiens conduits dans le cadre de ce mémoire.
[48] Centre de traitement des Appels/Centre Opérationnel Départemental d'Incendie et Secours.

- Le contrat entre l'Etat et la société EADS pour le maintien en condition opérationnelle d'ACROPOL arrive à son terme en 2012. Parallèlement, les SDIS ont des exigences en matière de garantie de temps de rétablissement (GTR) des liaisons d'ANTARES. La question des conditions du maintien en condition de l'INPT est posée.
- La DSIC (et ses services déconcentrés SZSIC et SDSIC[49]), est l'opérateur du réseau ACROPOL/ANTARES. Les SDIS étaient jusque là les opérateurs de leurs réseaux. Quant à la gendarmerie, elle reste opérateur de son réseau RUBIS. La question de l'opérateur de l'INPT se pose à l'horizon 2012. Opérateur privé avec mission de service public ? Opérateur d'Etat ? Plusieurs opérateurs ?
- Les SDIS ne sont pas interconnectés avec les réseaux intranet de messagerie des services de l'Etat. Le « portail ORSEC » est une remarquable exception à cet égard.
- Le débit offert par la technologie TETRAPOL est équivalent à celui du minitel. Ce faible débit résulte d'un choix privilégiant une infrastructure résistante et laissant à chaque utilisateur le soin de choisir en fonction de ses besoins, une des solutions hauts débits proposées par les opérateurs commerciaux. La plupart des utilisateurs estiment que ces besoins (flux vidéo, cartographie…) qui font l'objet d'applications grand public, doivent pouvoir intégrer le réseau interopérable et sécurisé de l'INPT. La technologie de l'INPT doit évoluer notamment en matière de débit.
- L'INPT attire de nouveaux utilisateurs potentiels : les services « routes » des conseils généraux, les douanes, l'armée de l'air, les polices municipales… Des critères d'accès doivent être établis.

Progressivement, les SDIS intègrent l'INPT. Mais quel est leur état d'interopérabilité ?

1.2.3 Etat d'interopérabilité des SDIS

Le SI intégré de l'établissement public

Comme la plupart des administrations et des entreprises, nombre de SDIS[50], développent l'interopérabilité à l'intérieur de leur organisation par le biais de la conception d'un SI global intégré.
Liés à une stratégie de l'établissement public, ce sont des projets importants, sur plusieurs années, qui nécessitent une maîtrise d'ouvrage forte.
Les modules d'applications informatiques de chaque service – ou briques logicielles - sont mis en réseau au moyen d'interfaces. La donnée est saisie par le service gestionnaire. Elle est contrôlée, mise en forme interopérable par un système intégrateur (middleware ou bus « intergiciel ») et stockée dans un unique « entrepôt de données » (datawarehouse). De là, elle peut être partagée et utilisée par les applications des autres services.
Cette urbanisation est garante de l'intégrité des données (pas de doubles saisies, pas de pertes d'informations, …).
Elle permet l'exploitation de tableaux de bord et d'indicateurs de gestion en temps réel donnant par là même aux décideurs une plus grande finesse et réactivité dans le pilotage du SDIS.

Dans ce type d'organisation, le système d'aide à la décision (SIAD) du CTA-CODIS constitue une composante (un module) intégrée au SI global de l'établissement.

[49] Direction des Systèmes d'Information et de Communication. Service Zonal des Systèmes d'Information et de Communication. Service Départemental des Systèmes d'Information et de Communication.
[50] C'est le cas, par exemple, des SDIS de la Gironde (33) et des Pyrénées Atlantiques (64) avec qui j'ai pu m'entretenir de ces questions.

L'interconnexion des SIC opérationnels : un processus qui démarre

La quasi-totalité des SDIS sont dotés d'un SIAD - ou SIC - pour la gestion opérationnelle[51].

Pour évaluer leur état d'interopérabilité, il semble pertinent de retenir trois indicateurs :

- le premier, est l'existence d'un lien avec le Centre de Réception et de Régulation des Appels (CRRA) du SAMU (plate-forme « physique » ou « virtuelle ») ;
- le second, est l'existence d'un système d'information géographique (SIG). En effet, le SIG fournissant à la base un ensemble de fonds de cartes vectorisés stimule le besoin d'enrichissement en données « métiers » utiles à la conduite des opérations (prévision). Cet enrichissement passe par des collectes sur le terrain mais aussi par des partenariats visant à mutualiser le partage des données. Cette démarche s'inscrit dans l'amélioration de l'interopérabilité des SIC ;
- le troisième, est le fait d'avoir réalisé ou prévu de réaliser l'intégration des fonctionnalités ANTARES dans le système de gestion opérationnelle.

Le tableau suivant résume ces indicateurs par catégorie de SDIS[52] :

indicateurs	Sur 18 SDIS 1ère catégorie	Sur 23 SDIS 2ème catégorie	Sur 24 SDIS 3ème catégorie	Sur 18 SDIS 4ème catégorie	Sur 11 SDIS 5ème catégorie	**% sur un total de 94 SDIS**
Existence d'une plateforme 15/18 ou projet en cours	6	11	10	6	3	**38% (12 réalisées et 24 projetées)**
Existence d'un SIG	13	10	16	14	8	**65%**
Intégration des fonctionnalités ANTARES (2005-2015)	11	17	15	13	7	**67%**

Bien qu'encore minoritaires, le nombre de projets de plates-formes 15/18 qui sont en cours de réalisation exprime une évolution dans ce sens.
Le fait que 2/3 des SDIS possèdent un SIG et que la même proportion a prévu d'intégrer les fonctionnalités ANTARES sont des signes de développement de l'interopérabilité.

Toutefois, les SIC des SDIS sont encore loin d'être interopérables avec ceux d'autres organisations.

La France n'est pas la seule à déployer un réseau national de radiocommunication numérique. Elle suit en cela une dynamique lancée au niveau européen.

[51] Sur 94 SDIS, 6 SDIS ne seraient pas équipés. Il est à noter par ailleurs que 23 SDIS déclarent ne pas avoir de CODIS permanent (*données INFOSDIS 2008*).
[52] Données INFOSDIS 2008.

1.2.4 Les réseaux nationaux de radiocommunication numériques partagés de cinq pays européens

En 1998, les accords de Schengen créent un espace de liberté, de sécurité et de justice à l'intérieur des frontières de l'Union Européenne (UE). Ces accords sont à l'origine d'un véritable contexte d'interopérabilité. Les différents pays de « l'espace Schengen » doivent harmoniser leurs pratiques et coopérer étroitement, notamment en matière de sécurité.
Dans le domaine des communications, la bande des 380/400MHz a été réservée pour les forces de sécurité publique et civile. Les technologies TETRA et TETRAPOL sont utilisés par les pays européens[53] qui déploient des réseaux nationaux au bénéfice de leurs forces de sécurité et de secours[54].
L'argument économique n'est pas en reste. Les NTIC entraînent des investissements lourds, aussi, le fait de remplacer les réseaux analogiques « vieillissants et dépassés » que détenait chaque service par un réseau unique partagé, permet de réaliser des économies d'échelle importantes.

Nous examinerons la situation dans cinq pays européens choisis pour leur représentativité en termes de choix et de modèles d'organisation. Ces cinq pays sont : l'Angleterre, la Belgique, la Suisse, l'Espagne et la Finlande.

Angleterre

Le gouvernement anglais a investi 1 milliard de livres (environ 1,1 milliard d'euros) dans un programme intitulé : Fire and Resilience Program (FRP) (Programme Résilience et Incendie)[55].
L'objectif de ce programme est de doter les services de secours d'urgence (police, pompiers, « ambulance service ») d'une réelle capacité de résilience, pour répondre en continu au risque courant quotidien comme aux accidents de portée régionale jusqu'aux catastrophes d'ampleur nationale (risques majeurs naturels et technologiques, actes de terrorisme).

Le FRP comprend 3 projets :

- New Dimension[56] : une dotation d'équipements spécialisés pour les pompiers (sauvetage déblaiement, NRBC[57], pompes de grand débit pour inondations ou grands feux, …).
- Firelink[58] : le déploiement d'un réseau de radiocommunication numérique sécurisé (TETRA) commun à l'ensemble des services d'urgence. Comme pour ANTARES en France, il s'agit d'une extension aux sapeurs pompiers du réseau AIRWAVE utilisé par les services de police et d'ambulance. L'ensemble des sapeurs pompiers aura rejoint le réseau en 2010.
- FiReControl[59] : un réseau de 9 centres opérationnels régionaux de régulation et de réception des appels[60] capable de mobiliser l'ensemble des moyens sapeurs pompiers au niveau national.

[53] Il est à noter que ce sont plutôt les pays du nord de l'Europe, notamment scandinaves, qui sont en avance dans ces domaines. Au palmarès 2008-2009 des pays les plus ouverts aux NTIC, on trouve 6 pays du nord de l'Europe aux 10 premières places (Danemark : 1er, Suède : 2ème, Finlande : 6ème, Islande : 7ème, Norvège : 8ème, Pays-Bas : 9ème. La France est au 19ème rang juste devant l'Allemagne et derrière l'Estonie). (http://www.weforum.org/pdf/gitr/2009/Rankings.pdf).
[54] TETRA et TETRAPOL sont deux technologies différentes de la société EADS. A terme, leur interopérabilité doit être assurée pour constituer un vaste réseau européen.
[55] http://www.communities.gov.uk/fire/resilienceresponse.
[56] Littéralement : « Nouvelle Dimension ».
[57] Nucléaire Radiologique Biologique Chimique.
[58] Littéralement : « Lien Incendie ».
[59] Littéralement : « Régulation Incendie ».

Le projet FiReControl semble particulièrement intéressant. En effet, il s'agit de remplacer au niveau des comtés[61] (counties) les équivalents de nos CTA/CODIS départementaux par des centres régionaux : les Regional Control Centers (RCC)[62].
Ces 9 centres seront reliés à 3 entrepôts de données nationaux et seront équipés de SIC très proches de ceux des CODIS (localisation de l'appelant, SIAD, géolocalisation des moyens, terminaux embarqués, etc.).

Les principaux avantages annoncés sont :

- la réalisation d'économies structurelles (9 centres au lieu de 46) ;
- la sécurité par redondance (les 9 centres sont en réseau) ;
- la centralisation des informations par la mise en place d'un SI global au niveau national ;
- l'interopérabilité, gage d'une meilleure efficacité opérationnelle.

Le projet se heurte actuellement à des difficultés de réalisation d'ordre technique. La bascule des 46 centres opérationnels des comtés vers les 9 centres régionaux vient d'être repoussée de plusieurs mois et devrait commencer au printemps 2011 pour s'achever fin 2012.
Il y a aussi des oppositions. Ainsi le principal syndicat de sapeurs pompiers anglais est en désaccord avec le choix du niveau régional pour la conduite des opérations qui se fait actuellement au niveau du comté. Enfin il est à noter que l'Ecosse et le Pays de Galles ne se sont pas associés au projet.

Le FRP est un programme ambitieux qu'il convient de suivre pour en tirer des enseignements car il possède des similitudes avec des initiatives récentes du gouvernement français (dotations d'équipements NRBC et INPT).

Belgique

Le gouvernement belge a opté pour un réseau de radiocommunication sécurisé (TETRA) commun à tous les services de secours et de sécurité. En juin 1998, la société anonyme de droit public ASTRID[63]est créée. Trois domaines sont couverts :

- le réseau radio. Il comprend 500 stations de base réparties sur l'ensemble du territoire belge. Il est développé par province[64].

- Le réseau paging. C'est le réseau d'appel des forces d'intervention qui utilise l'infrastructure du réseau radio.

- Le dispatching CAD. Il s'agit de systèmes d'aide à la décision pour la réception des appels[65], les radiocommunications et l'exploitation de base de données opérationnelles. Ces systèmes équipent les 11 Centres d'Information et de Coordination[66] (CIC) de la police. Vieillissants, les centres « 100 » des sapeurs pompiers sont destinés à migrer sur le système CAD. A terme, il est prévu de mettre en place des plates-formes communes pour réceptionner le 112 (aide médicale urgente, police, pompiers) en remplacement du 100 et du 101. Dans

---

[60] Le 999, équivalent de notre 18.
[61] Les comtés peuvent être comparés territorialement à nos départements.
[62] L'équivalent en France, serait un CTA /CODIS/COZ au niveau zonal ou régional.
[63] All-round Semi-cellular Trunking Radio communication system with Integrated Dispatchings**.**
[64] La Belgique a 10 provinces.
[65] Le 101 est le n° d'appel d'urgence de la police (équivalent à notre 17) et le 100 celui des pompiers (équivalent à notre 18).
[66] Un par province et un pour la région de Bruxelles-Capitale.

un deuxième temps, il est envisagé de dissocier la fonction « gestion des appels » confiée à des préposés « neutres », de la fonction « gestion et suivi des opérations » effectuée par chaque service impliqué (police, pompier).

La société ASTRID est chargée d'opérer le réseau et de fournir tous les équipements. En contrepartie, elle perçoit un abonnement auprès de chaque service utilisateur.
Les utilisateurs d'ASTRID sont tous les services impliqués dans la protection des populations. Un comité des 15 utilisateurs principaux donne un avis sur les candidatures d'entreprises privées souhaitant intégrer ASTRID. Celles-ci doivent jouer un rôle en matière de protection des populations.
Il conviendra d'observer la mise en place de centres dédiés à la réception des appels dissociés des centres de gestion opérationnelle, afin d'en tirer des enseignements.

Suisse

POLYCOM est le sigle du réseau radio suisse de sécurité (TETRAPOL). Il fournit une infrastructure de communication homogène à l'ensemble des Autorités et des Organisations chargées du Sauvetage et de la Sécurité (les AOSS)[67] au niveau fédéral, cantonal et communal.
Le réseau POLYCOM est formé d'un ensemble de sous réseaux mis en place par les cantons pour répondre à leurs besoins en tenant compte des prescriptions fédérales. D'ici fin 2012, il couvrira avec environ 760 relais la totalité de la Suisse pour un investissement d'environ 480 millions d'euros.
Le financement du projet POLYCOM est assuré à environ 65% par la confédération suisse. De plus, la confédération donne aux cantons un montant forfaitaire pour la maintenance. Le reste des coûts doit être supporté par le canton.
Chaque canton, par l'intermédiaire des services techniques de sa police cantonale, est opérateur de réseau (soit 24 opérateurs). Par ailleurs, chaque canton dispose d'une cellule de crise.
POLYCOM veut laisser à des entreprises tierces la possibilité de proposer des produits. Dans cette optique, ainsi que pour le développement de solutions techniques futures, POLYCOM a ouvert le marché en définissant avec son partenaire SIEMENS, chargé de l'intégration, des interfaces normalisées sur lesquelles les entreprises doivent adapter leurs produits.
POLYCOM est coordonné par une direction de projet rattachée à l'OFPP (Office Fédéral de la Protection de la Population). Cette direction pilote le groupe de travail « utilisateurs POLYCOM » composé de représentants de chaque organisation. C'est dans ce groupe que sont prises 4 fois par an, toutes les décisions concernant POLYCOM. Le groupe « utilisateurs » établit un document de conditions et de prescriptions qui définit les règles (organisation, techniques, et financières) que chaque utilisateur et opérateur doivent respecter. Il prend également position sur les différentes demandes des cantons ou organisations.
Il est à noter que, comme en France avec le SIAP et ANTARES, il est envisagé d'utiliser le réseau POLYCOM pour commander les quelques 8000 sirènes d'alarme à la population.

Le système suisse se distingue par le nombre très large de services utilisateurs. Là aussi, les entreprises privées manifestent leur intérêt.
Au contraire de la Belgique, la Suisse a fait le choix de laisser chaque canton opérer son réseau.

[67] Les AOSS sont : le corps des gardes frontières, les polices (cantonales et municipales), l'armée (sécurité militaire, police fédérale, services militaires spéciaux (pompiers militaires, etc.)), la protection civile, les pompiers, la santé (ambulances, service de secours héliportés), d'autres services (entretien des routes, prisons, centrales électriques, …)

La démarche de normaliser des interfaces pour permettre à toutes les entreprises intéressées de développer des applications mérite d'être suivie.
Enfin, sont à l'étude des solutions techniques permettant de s'affranchir des limites en débit du réseau pour répondre aux besoins de data « lourdes » (vidéo, cartographie) exprimés par les utilisateurs.

Espagne

Le réseau commun espagnol s'appelle SIRDEE[68] (TETRAPOL). Il est partagé par la Guardia Civil et la police nationale. 1450 relais sont déployés au niveau des 52 provinces que compte l'Etat espagnol. A terme, il doit intégrer les organisations ou services suivants : surveillance du trafic routier, communautés autonomes (au nombre de 17), la protection civile, les pompiers et les polices municipales.
L'Espagne a confié la réalisation du réseau SIRDEE à Telefonica, un grand opérateur de télécommunication (comparable à France Telecom). Telefonica est propriétaire du réseau et des terminaux dont il assure la maintenance. Les utilisateurs lui versent une redevance. A la fin du contrat, l'Etat reste propriétaire des terminaux.

Dans le modèle espagnol (comme pour l'Angleterre et la Belgique), les termes et la durée du contrat sont essentiels pour garantir d'une part, les exigences techniques des utilisateurs et d'autre part, protéger le contribuable. Une comparaison à ce sujet réalisée entre SIRDEE (Telefonica) et le réseau anglais AIRWAVE (O2) montre des différences notables[69].

Finlande

VIRVE (TETRA) est le réseau national numérique partagé de la Finlande.
Imaginé dans les années 80, il est opérationnel depuis 2002. VIRVE a remplacé une cinquantaine de réseaux radio analogiques et il est estimé que son coût représente 20 à 30% de ce qu'il aurait fallu dépenser s'il avait fallu remplacer chaque réseau séparément.
Le coût d'investissement, pris en charge par l'Etat, s'élève à 200 millions d'euros. Les coûts de fonctionnement sont d'environ 20 millions d'euros par an dont la moitié est prise en charge par l'Etat. L'autre moitié est prise en charge par les utilisateurs sur la base d'un abonnement de 30 euros par mois et par terminal.
Le propriétaire et opérateur du réseau VIRVE est la Suomen Erillisverkot Oy, une société détenue par l'Etat finlandais, qui est également en charge de tous les réseaux de sécurité des agences gouvernementales.
VIRVE a développé les liens de coopération entre les différents services et agences de sécurité et a donné une nouvelle dimension à la sécurité nationale.
Les utilisateurs principaux du réseau sont les services de secours et de sécurité de l'Etat et des communes : services de secours et d'incendie, police, services sociaux et de santé, douanes, forces de défense, … Il est à noter que le combiné VIRVE est interopérable avec les réseaux de téléphonie fixe et mobile simplifiant la tâche des utilisateurs.
La mise en place pour tout le pays, d'un centre unique de réception des appels et de gestion opérationnelle est une des applications la plus remarquable liée à VIRVE. L'Emergency Response Centre[70] (ERC) a remplacé les centaines de centres de réception locaux préexistants et gère le 112, numéro unique pour l'urgence.

[68] « SIstema de Radiocomunicationes Digitales de Emergencia del Estado ».
[69] Cette comparaison montre les coûts supérieurs du modèle anglais (*in* http://www.docstoc.com/docs/2410137/SIRDEE-AIRWAVE-Study-of-the-Impact-of-the-choice-between-TETRAPOL).
[70] Littéralement : « Centre de Réponse de l'Urgence ».

L'appel au 112 permet d'obtenir l'intervention des services suivants : ambulance, police, pompiers, secours maritimes, services sociaux et autres services similaires. Le déclenchement opérationnel est assuré par le système VIRVE.
L'ERC réceptionne annuellement près de 4 millions d'appels dont environ la moitié est transmis aux différents services d'urgence pour traitement. 47% sont liées aux ambulances, 46% relèvent de la police et 7% des secours.

Le réseau fournit le vecteur nécessaire aux interconnexions. En cela, il est structurant pour les organisations mais est-il adapté au modèle d'organisation de la sécurité civile ?

1.2.5 Au cœur des orientations de la politique de sécurité civile

« Les orientations de la politique de sécurité civile[71] » décrivent ce vers quoi doit tendre l'organisation de la sécurité civile. Nous trouvons dans ce texte un certain nombre de mots et de concepts révélateurs.

Tout d'abord, dans le préambule de ce document, nous trouvons l'expression de la nécessité d'une **diversité des acteurs** qui est devenue une caractéristique de la sécurité civile.
Face à la menace terroriste, les services de secours sont amenés à **participer** au dispositif d'**ensemble** de la sécurité intérieure.
L'**implication** de chaque citoyen dans la sécurité civile nécessite un **engagement** et le développement d'une **culture** de la **préparation** au risque et à la menace.
Les orientations ont deux caractéristiques : elles sont **volontaristes** et « *imposent une* ***coordination dépassant les frontières*** *habituelles des services, de leurs attributions et de leurs prérogatives, pour mieux les* ***faire travailler ensemble*** ».

Les orientations se déclinent selon 3 axes.

Le premier axe prône de s'**attaquer** aux risques en les **anticipant**. Il faut **connaître**, **prévoir** et se **préparer**.
Les recommandations en matière de connaissance des risques équivalent à une **mise en réseau** de toutes les compétences requises. C'est un véritable **travail collaboratif** qui est proposé à travers la mise en place d'un conseil national de la sécurité civile présidé par le Ministre de l'Intérieur et prolongé au niveau local par les conseils départementaux placé auprès de chaque préfet. Pour chaque risque, un ministère est désigné comme **chef de file**.
En matière de planification, l'**élaboration en commun** par tous les acteurs concernés de scénarios centrés sur l'action ainsi que le **partage** d'un répertoire commun des risques sont de mises.
Le passage de l'exercice à l'entraînement implique « *non seulement les autorités publiques et les services de secours, mais aussi la population* ». Le **partage** et la diffusion à tous, de retours d'expérience **pluridisciplinaires**, élaborés par des évaluateurs indépendants doivent être améliorées.

Dans le deuxième axe, il est question de refonder la notion de protection des populations en confirmant que « *la* ***personne secourue*** *est au cœur de toute politique de sécurité civile* » et en misant sur le comportement de « *citoyens* ***informés*** *et* ***responsables*** », capables de s'intégrer dans des dispositifs **collectifs** de réponse.
La veille opérationnelle et l'alerte se structure autour de la **circulation** de l'information.

---

[71] Approuvées par l'article 3 de la loi n° 2004-811 du 13 août 2004 de modernisation de la sécurité civile, elles figurent en annexe de la dite loi.

La mobilisation de tous les moyens en **organisant** la réponse à l'événement constitue le troisième axe qui clôt les orientations de la politique de sécurité civile. L'organisation française éprouvée du **commandement unique** est confirmée avec ses deux « étages » : « *le maire pour le secours de proximité, le représentant de l'Etat pour les sinistres de grande ampleur* ». De même est confirmé, le principe de **gratuité** des secours.
L'accent est mis sur la nécessaire modernisation et **rationalisation** des plates-formes opérationnelles et des postes de commandement.
La **répartition** des compétences et des responsabilités entre l'Etat, les départements et les communes mais aussi les associations, les moyens privés et les opérateurs de services publics est abordée dans un souci de clarification, de simplification et de **complémentarité**, ceci dans le **respect** des principes d'organisation générale.

Les orientations de la politique de sécurité civile décrivent une organisation dont les valeurs correspondent à une organisation en réseaux : solidarité, tolérance, transparence, ouverture, confiance, dynamisme, efficience, ces valeurs s'appuient sur les notions d'égalité, d'équité, de performance et de cohérence.

L'organisation en réseaux apparaît donc comme adaptée à l'organisation « sécurité civile ».

Elle permet de faire travailler ensemble les différents acteurs qui partagent la même mission : la protection des populations.

2 METTRE EN RESEAU LES DIFFERENTS ACTEURS CONCOURANT AUX MISSIONS DE SECURITE CIVILE *(« In varietate concordia »)*[72]

2.1 La nécessité d'une vision partagée

2.1.1 Un contexte à exploiter

Les entraînements multiservices

Chaque acteur de la sécurité civile possède, dans son domaine de compétence, des savoir-faire reconnus et des moyens adaptés.

Cependant, face aux risques et aux menaces d'ampleur qui nécessitent une réponse coordonnée de l'ensemble des services, ceux-ci sont insuffisamment préparés.
La menace d'attentats terroristes NRBC figure en première place dans la hiérarchisation des risques et des menaces pour le territoire national[73].

S'entraîner sur ce type de menace est particulièrement pertinent dans le cadre d'un travail sur l'interopérabilité. En effet, un tel scénario exige des différents protagonistes un partage et un échange rapide d'informations de la plus haute importance et ce, dès les premiers instants de la crise (zone touchée, population concernée, météo, nombre de victimes estimée, qualification du risque NRBC, conduites à tenir, etc.).

Les retours d'expérience actuels de ces exercices[74] ne débouchent pas sur des enseignements concrets en termes d'interopérabilité technique et d'interopérabilité des doctrines.

Une évaluation ciblée « réseaux » permettrait de mettre en évidence les besoins d'interfaces entre les SI des différents acteurs pour le partage et l'échange d'informations et de travailler sur les critères de celles-ci (nature, forme, circuits de diffusion, etc.).

Une évaluation ciblée « procédures » permettrait de développer chez tous les acteurs une culture commune de la gestion de crise par l'emploi d'outils et de concepts identiques. Un référentiel commun des doctrines pourrait être établi sous le pilotage de l'acteur « chef de file ».

Les modes d'évaluation des entraînements de crise pourraient être confiés à un ou plusieurs experts indépendants[75] désignés par l'Etat.

Le chef de file serait l'acteur le mieux placé en termes de savoir-faire et de moyens.

La RGPP

Dans le cadre de la révision générale des politiques publiques (RGPP), la réforme de l'administration territoriale de l'Etat vise à une meilleure performance de la politique publique (de meilleures prestations à un moindre coût).

---

[72] « Unité dans la diversité », devise de l'Union Européenne.
[73] Livre Blanc de la Défense et de la Sécurité nationale (2008 :59).
[74] MetroTox Lyon 2004, Euratech 2005, MetroTox Marseille 2005, etc.
[75] Par exemple, des experts de la Fondation pour la Recherche Stratégique (FRS).

L'amélioration de la performance des services doit être obtenue notamment par la clarification de l'organisation et par le développement des mutualisations à tous les niveaux, en particulier pour les fonctions support[76].

Cette réforme se traduit par un regroupement des directions au niveau régional et départemental.

Au niveau départemental, les nouvelles directions interministérielles se mettent en place autour d'une architecture mutualisée d'un SIC, par nature transversal.
Un correspondant SIC interministériel est nommé dans chaque département sous le pilotage d'un comité national réunissant les DSI des ministères.

La mutualisation des infrastructures et des outils est recherchée dans les domaines suivants :

- infrastructures (réseaux) et téléphonie ;
- infrastructures d'authentification locale ;
- sécurité des systèmes d'information (SSI) ;
- messagerie/annuaire ;
- Intranet/Internet ;
- SIG.

Cette mise en cohérence favorise l'interopérabilité interne des services déconcentrés de l'Etat. Elle fournit également une opportunité à saisir pour relier le nouveau SIC avec certains SIC « extérieurs » (pompiers, police, gendarmerie, SAMU, mais aussi, opérateurs, services « routes », santé et environnement des collectivités territoriales).

La méthode de travail retenue sous l'égide de la MIRATE[77] en matière d'unification des SIC des services déconcentrés de l'Etat pourrait être utilement étendue aux services décentralisés concourant à la sécurité civile, dans un objectif de maîtrise de l'information en situation de crise.

Les enseignements tirés des crises : L'exemple de KLAUS

Le 24 janvier 2009, à 5h00 du matin, l'ouragan KLAUS s'abattait sur le sud-ouest de la France.
En quelques heures, le département des Landes se retrouvait sans réseaux de communications (routes et trafic SNCF coupés) et sans électricité entraînant en cascade la perte de l'alimentation en eau potable et de la téléphonie mobile.
La crise a duré 3 semaines nécessitant la coordination d'importants moyens humains et matériels (2000 hommes, militaires et sapeurs-pompiers, plus de 3000 agents d'ERDF, des milliers de groupes électrogènes…).

A la faveur de cette expérience, nous pouvons tenter une représentation sous forme de tableau, des 5 domaines d'informations nécessaires à un Poste de commandement (PC) de crise.

[76] Circulaire du 7 juillet 2008 relative à l'organisation de l'administration départementale de l'Etat. Les SIC sont explicitement désignés comme faisant partie du champ des mutualisations des fonctions support.

[77] Mission Interministérielle pour la Réforme de l'Administration Territoriale de l'Etat.

Domaines	Nature d'informations	Outils/Ressources
Environnement, aménagement du territoire et gestion des risques	Toutes les informations décrivant l'espace de la zone d'intervention : informations géo référencées de type cartographique (topographie) enrichie des données « métiers » des services chargés de l'aménagement du territoire et de la gestion des risques (population, ERP, crues de référence, catégories de routes, réseaux d'énergie, réseaux d'eau, maisons de retraite, industries « vitales », etc.). Données de prévention, prévision, planification, scénarii.	« Couches » des données « métiers » des services gestionnaires pouvant intégrer le SIG du PC de crise ou être accessibles par un portail web. Les services les plus importants doivent être représentés au PC de crise.
Cinétique des événements	Données météo (vent, précipitations, degré hygrométrique), messages remontant du « terrain », données issues de capteurs (montée des eaux, état de la végétation, détection des départs de feux, …) exploitées par des outils de modélisation sur SIG décrivant des situations envisageables à T+…	Capteurs des services chargés de la veille et des paramètres en temps réel ; remontées de l'information ; logiciels de modélisation existants ou à développer ; Carte projetée actualisée des situations
Moyens/Ressources par rapport aux Besoins/Manques	Etat des forces/capacités et des faiblesses/besoins confrontés aux menaces/opportunités de l'environnement décrit par les 2 domaines précédents	Outils de bureautiques pour la gestion des moyens et des ressources ; matrices d'aide à l'élaboration de stratégies
Conduite opérationnelle	Boucle : situations, actions, anticipation, commandement/transmissions, sécurité, évaluations	Outils des services opérationnels
Communication de crise	Indicateurs choisis issues des domaines précédents : situation, objectifs, missions, effectifs, matériels, progression, difficultés, …	« Grille » de communication pouvant faire l'objet d'un développement informatique. Medias de service public.

« *Actuellement, il n'existe pas de représentation consolidée de la situation opérationnelle sur l'ensemble d'un département*[78] ».

Cependant, toutes ces données et ces outils existent. Tout l'enjeu réside dans leur mise en relation pour aboutir à un SI de gestion de crise[79].

[78] « *Prospective sur les systèmes d'information et de commandement pour la sécurité intérieure (Etude de cas des Yvelines)* », juillet 2009, Délégation à la Prospective et à la Stratégie, Ministère de l'Intérieur.
[79] Il faut s'intéresser aux travaux de l'OTAN sur les systèmes COP (Common Operational Picture ou modèle commun opérationnel).

La Directive INSPIRE[80]

Le système d'information géographique est au service de la connaissance et de la gestion des territoires, de la gestion de crise, de la gestion et de la prévention des risques et de l'aide à la décision. Il constitue un espace d'organisation entre les métiers et facilite le travail multiservices.
En représentant l'espace selon des standards reconnus par tous, la cartographie est le support universel du partage de l'information, particulièrement utile en situation de crise.

Le 15 mai 2007, la Directive européenne INSPIRE entre en vigueur. Elle vise à fixer « *les règles générales destinées à établir l'infrastructure d'information géographique dans la Communauté européenne aux fins des politiques environnementales communautaires et des politiques ou des activités de la Communauté susceptibles d'avoir une incidence sur l'environnement* [81]».

Elle introduit les principes suivants[82] :

- constituer un **catalogue**, afin qu'il soit aisé de rechercher les données spatiales disponibles, d'évaluer leur adéquation et de connaître les conditions applicables à leur utilisation ;
- appliquer le principe de **subsidiarité**, pour que les données soient stockées, mises à disposition et entretenues au niveau le plus approprié ;
- garantir l'**interopérabilité** des données par le respect de normes internationales[83], afin qu'il soit possible de combiner des données spatiales de différentes sources d'une manière cohérente et de les partager entre plusieurs utilisateurs et applications ;
- instituer le **partage** des données spatiales, collectées à un niveau d'autorité publique puis partagées à tous les niveaux d'autorité publique ;
- permettre l'**accès** aux données spatiales par des mises à disposition dans des conditions qui ne fassent pas obstacle à leur utilisation extensive ;
- utiliser le réseau **Internet** comme vecteur central avec la mise en place de services en ligne pour effectuer toutes les opérations (sites de portails).

La Directive INSPIRE s'intéresse aux données géographiques numériques détenues par des autorités publiques. Les thèmes de données sont définis et font l'objet de 3 annexes : les données de référence (annexes I et II) et les données environnementales (annexe III)[84].
La Directive va être transposée dans le droit français en 2010. Le MEEDDM[85] est chargé de cette transposition. L'avant-projet de loi[86] vise à établir une infrastructure nationale de l'information géographique s'appliquant aux données détenues par les autorités publiques[87] et certains tiers.

Nous sommes tentés de faire un parallèle entre cette infrastructure et l'INPT. Toutes deux sont destinés à irriguer les SIC des acteurs concourant aux missions de sécurité civile.

---

[80] INfrastructure for SPatial InfoRmation in Europe.
[81] Article 1 de la Directive.
[82] « *La Directive INSPIRE en 10 points* », BRGM, mars 2009.
[83] ISO 19115, 19119, 19139.
[84] En annexe 2 de ce mémoire.
[85] Ministère de l'Ecologie, de l'Energie, du Développement Durable et de la Mer.
[86] http://www.ign.fr/DISPLAY/000/527/990/5279901/Av-proj-loi_transp_INSPIRE.pdf
[87] Au sens de l'article L124-3 du code de l'environnement, c'est-à-dire : l'Etat, les collectivités territoriales et leurs groupements, les établissements publics, les personnes chargées d'une mission de service public en rapport avec l'environnement.

Les initiatives régionales et zonales en matière de SIG

La France a accumulé un retard en matière numérique. Elle vise à se replacer parmi les grandes nations numériques à l'horizon 2012. Le Plan de Développement de l'Economie Numérique, lancé en 2008, prône une gouvernance transversale des SI de l'Etat. Il préconise la mise en place de référentiels communs favorisant l'interopérabilité entre administrations[88].

La circulaire PRODIGE[89] du 24 octobre 2007 fait du développement des SIG dans les services de l'Etat en région, un axe stratégique de la modernisation de l'administration. Elle identifie la région comme le niveau pertinent d'interopérabilité des SIG territoriaux. Dans un esprit de partenariat visant à mutualiser l'acquisition des données et leur partage sous un format interopérable, plusieurs initiatives couronnées de succès ont vu le jour. Citons le SIG PRODIGE de la région Rhône-Alpes, le SIG Littoral, le SIG de la Zone de Défense Sud, le projet PIGMA[90] dans la Zone de Défense Sud-Ouest.

Le projet PIGMA se distingue des autres en ce sens qu'il ne repose pas sur une structure de l'Etat mais sur un partenariat original : le GIP_ATGeRI[91].
Constitué le 28 octobre 2005, le GIP_ATGeRI regroupe l'Etat (MEEDDM, Ministère de l'Agriculture et Ministère de l'Intérieur), les SDIS de la Dordogne, de la Gironde, des Landes, du Lot-et-Garonne et des Pyrénées Atlantiques, l'ARDFCI[92] et les Unions des ASADFCI[93] ainsi que l'ONF[94].

Le projet PIGMA a pour objectifs principaux :

- de favoriser l'interopérabilité entre les services,
- d'impulser une dynamique régionale de partage autour d'outils d'aide à la décision en complément des actions locales,
- de générer une économie d'argent public par la mutualisation des achats et des moyens.

La cohérence de l'ensemble des projets de mutualisation de l'information géographique se fera à travers la transposition dans le droit français de la Directive INSPIRE. Le respect des règles d'interopérabilité permettra aux différents projets territoriaux de « s'emboîter » pour constituer un ensemble national et européen.

Le besoin en information géographique est général à tous les niveaux d'utilisateurs. Ceci explique la dynamique de ces projets et l'adhésion volontaire des divers acteurs. réunis sur ces projets ,.

Participer à de tels projets, générateur d'échanges et d'économies, dans le cadre de la déclinaison de la Directive INSPIRE est une opportunité à saisir pour les acteurs concourant aux missions de sécurité civile.

Pourquoi ne pas ajouter au catalogue de l'information géographique un thème relatif aux données de sécurité civile ?

---

[88] Citons à cette occasion, le référentiel général d'interopérabilité (RGI) visant à l'interopérabilité des documents électroniques.
[89] Plate-forme Régionale pour Organiser et Diffuser l'Information Géographique de l'Etat.
[90] Plate-forme de l'Information Géographique Mutualisée en Aquitaine.
[91] Le Groupement d'Intérêt Public d'Aménagement du Territoire et Gestion des Risques. Voir Annexe 3 de ce mémoire.
[92] Association Régionale de Défense des Forêts Contre l'Incendie.
[93] Associations Syndicales Autorisées de DFCI.
[94] Office National des Forêts.

2.1.2 Des faiblesses à combler

Villages gaulois

En forçant le trait, le constat négatif suivant pourrait être dressé :

- La police a tendance à considérer que les problèmes de sécurité intérieure priment et que le reste doit en découler ;
- La gendarmerie a tendance à considérer qu'elle se suffit à elle-même et qu'elle détient toutes les solutions à tous les problèmes ;
- Les SAMU sont au service de la stratégie mise en place pour assurer le fonctionnement des hôpitaux ;
- Les SDIS sont divisés, centrés sur leurs problématiques locales et leurs relations avec leurs administrateurs, élus locaux ;

Tout le monde n'est pas convaincu des vertus de l'interopérabilité et de l'intérêt à interconnecter les services.
Il manque des référentiels partagés, un langage commun (doctrines, procédures, normes), une feuille de route.
Il manque un sentiment fort d'appartenance à une famille qui doit s'identifier autour des mêmes valeurs : la famille des acteurs concourant aux missions de sécurité civile.

Un manque de culture d'interopérabilité

Avec l'INPT et le développement des SI dans les organisations, les concepts de réseaux et d'interopérabilité font leur apparition. Les décideurs des équipes de direction mais aussi les hauts fonctionnaires de l'Etat et les présidents de CASDIS sont insuffisamment sensibilisés à ces questions.

Il n'existe pas d'enseignement abordant ces sujets, dispensé au sein des écoles des cadres supérieurs des principaux acteurs concourant aux missions de sécurité civile, qui favoriserait la promotion et la diffusion d'une culture des réseaux et de l'interopérabilité.

L'hétérogénéité administrative des acteurs

La diversité des acteurs et leur dispersion crée une difficulté pour identifier les axes de connexion et les bons niveaux d'interfaçage.

Au quotidien, les services du MEEDDM[95] « doublonnent » souvent avec les services de la DSC et des SDIS pour tout ce qui concerne la prévention et la gestion des risques. L'identification de ces « doublons » par ces acteurs leur permettrait d'appréhender un travail en commun basé sur la complémentarité des approches. Des partenariats pourraient être mis en place pour constituer des systèmes en réseaux notamment en matière d'analyse du risque et de planification[96].

Avec le rattachement cette année, de la gendarmerie au Ministère de l'Intérieur, l'Etat affiche une ligne claire en matière de sécurité intérieure. L'objectif de rapprochement entre la police et la gendarmerie est affiché dans un souci d'efficience.

[95] Ministère de l'Ecologie, de l'Energie, du Développement Durable et de la Mer.
[96] De tels partenariats ou réseaux informels existent ici ou là, reposant sur des initiatives locales ou de conjoncture.

Les autres acteurs de l'Etat dépendent de ministères différents (Santé, MEEDDM, Agriculture). En cas de crise touchant aux populations, le Ministre de l'Intérieur, chargé de la sécurité civile, a vocation à assurer le rôle de chef de file vis-à-vis des autres Ministères comme c'est le cas actuellement, pour la gestion de la grippe H1N1.

Pour le cœur de la sécurité civile, la DSC est rattachée au Ministère de l'Intérieur ainsi que les SDIS qui relèvent du préfet pour la partie opérationnelle.

Les services techniques des collectivités territoriales disposent de moyens importants participant aux crises de sécurité civile. De part leur position, les SDIS conventionnent ou mutualisent de plus en plus avec ces services[97].

Enfin, la disparition de structures des opérateurs de service public au niveau local est une source de difficulté. Il importe, dans un souci de cohérence, de lisibilité et d'efficacité en situation de crise que les structures des différents acteurs de la sécurité civile colle au plus prés du découpage administratif.

La réforme de l'administration territoriale de l'Etat et celle annoncée, des collectivités territoriales, sont l'occasion d'un réexamen possible de l'architecture de la sécurité civile.

Dans un tableau, représentons l'organisation structurelle des principaux services impliqués dans la sécurité civile aux différents échelons administratifs du territoire.

Acteurs/Niveaux	Commune, canton, arrondissement	département	Région, Zone de Défense	national
Police	Commissariat	DDSP		DGPN, Ministère de l'Intérieur
Gendarmerie	Compagnie, brigades	Groupement	Région	DGGN, Ministère de l'Intérieur
Pompiers territoriaux	Groupement, centre d'incendie et de secours	SDIS (CODIS)	EPIDIS[98] ?	CNSIS
Sécurité Civile d'Etat	-	Préfecture (COD)	Moyens zonaux, EMZ-COZ	Moyens nationaux, DSC, Ministère de l'Intérieur
Environnement – Equipement - Agriculture		Services déconcentrés	Directions régionales	MEEDDM, Ministère de l'Agriculture
SAMU	SMUR	Hôpitaux (SAMU)	ARS[99]	DHOS, Ministère de la Santé
Collectivités Territoriales	Services municipaux	Services Conseil Général	Services Conseil Régional	ARF, ADF, AMF
Opérateurs de service public		Délégations départementales (*pas partout*)	Délégations régionales	Directions

Ce tableau illustre les interfaces possibles aux différents niveaux entre les différents acteurs.

[97] Mutualisation de l'atelier départemental avec le service « routes » du Conseil Général, par exemple.
[98] Etablissement Pubic Interdépartemental d'Incendie et de Secours.
[99] Agence Régionale d'Hospitalisation.

Verticalement, il met en évidence deux niveaux « privilégiés » pour mettre en contact les différents acteurs sur des problématiques de sécurité civile : le niveau départemental et le niveau national[100].

La CNSIS : nouveau modèle de gouvernance[101] ?

Les SDIS, établissements publics départementaux, ont une double tutelle : le préfet, pour la partie opérationnelle et le président du Conseil Général (ou un élu désigné par lui) pour la partie administrative et financière.
Si les 100 SDIS[102] bénéficient de plus de souplesse et de réactivité par rapport à la « lourdeur » d'une organisation étatique, l'articulation avec le niveau national pose quelques difficultés.

La conférence nationale des services d'incendie et de secours (CNSIS) améliore sur ce point la gouvernance des SDIS et constitue un lieu favorable aux échanges[103].
Composée de membres des assemblées parlementaires, de représentants des sapeurs-pompiers volontaires et professionnels, de représentants de l'Etat et, en majorité, de représentants des conseils d'administration des services départementaux d'incendie et de secours, elle est consultée sur les projets de loi ou d'acte réglementaire relatifs aux missions, à l'organisation, au fonctionnement ou au financement des services d'incendie et de secours. Elle peut émettre des voeux[104].
Consultée sur le projet de décret traitant de l'INPT[105], l'orientation favorable qu'elle a donnée après débat, a « validé » l'adhésion des SDIS au réseau ANTARES.

La CNSIS est peut-être le modèle d'une future Conférence nationale des acteurs concourant aux missions de sécurité civile dont un des sous-groupes pourrait être en charge des SIC ?

Le programme ANTARES : axe du développement de l'interopérabilité

Le référentiel commun traitant de l'organisation du secours à personne et de l'aide médicale urgente[106] comporte une partie[107] relative aux « *évolutions et axes de progrès* » des « *systèmes de transmission et d'informatisation* ».
Cette partie peut être qualifiée de « manifeste de l'interopérabilité » et constitue une véritable feuille de route. L'interopérabilité est présentée comme « *l'axe stratégique commun de modernisation des systèmes d'information et de communication*[108] » des SDIS et des SAMU.
Cet axe se décline au travers du programme ANTARES qui « *constitue l'ossature technique nationale indispensable à la constitution de référentiels, d'outils et d'applications informatiques interopérables*[109] ».

---

[100] On ne peut s'empêcher de penser au Conseil National de la Sécurité Civile et au Conseil Départemental de la Sécurité Civile, *Orientations de la politique de sécurité civile, loi n° 2004-811 du 13 août 2004 de modernisation de la sécurité civile*.
[101] De manière générale, la gouvernance se définit comme « un processus de coordination d'acteurs, de groupes sociaux, d'institutions pour atteindre des buts propres discutés et définis collectivement dans des environnements fragmentés et incertains. » *Gouvernance des territoires et charte managériale*, CARLES J. 2007 :90.
[102] 93 en métropole et 7 outre-mer.
[103] Signalons également le sous-groupe de l'ADF constitué par les Présidents de SDIS et qui se réunit 2 fois par an.
[104] Article 44, loi n° 2004-811 du 13 août 2004 de modernisation de la sécurité civile.
[105] Décret no 2006-106 du 3 février 2006 relatif à l'interopérabilité des réseaux de communication radioélectriques des services publics qui concourent aux missions de sécurité civile.
[106] Arrêté du 24 avril 2009 relatif à la mise en œuvre du référentiel portant sur l'organisation du secours à personne et de l'aide médicale urgente (référentiel élaboré par le comité quadripartite associant les représentants des structures de médecine d'urgence et des services d'incendie et de secours, la DDSC et la DHOS ; date de parution : 25 juin 2008).
[107] Titre II, chapitre VI, partie A (pages 44 à 46).
[108] *Ibid*.
[109] *Ibid*.

« *Les référentiels techniques d'interopérabilité doivent être complétés par un référentiel d'exigences communes sur la performance et la qualité opérationnelle fournie par les systèmes d'information des SAMU et des SIS* [110]». Cette démarche doit aller au-delà du périmètre ANTARES pour être « *étendue à l'ensemble des systèmes d'information et de communication qui constituent la réponse des services publics à une demande de secours, depuis la réception de l'appel jusqu'à la fin de l'intervention*[111] »

Au final, il s'agit de faire travailler ensemble les deux acteurs majeurs en matière de secours et de soin urgent : « *En exploitant ANTARES conformément aux référentiels techniques d'interopérabilité, les systèmes d'information des SIS et des SAMU doivent permettre la collaboration entre CRRA et CODIS eux-mêmes ou bien sur le terrain entre un chef d'agrès et un CRRA ou encore entre un SMUR et un CTA-CODIS*[112] ».

Ce travail engagé constitue un véritable test pour le développement de l'interopérabilité au niveau national entre les acteurs concourant aux missions de sécurité civile.

ANTARES sera t-il l'outil qui décloisonnera les organisations ?

De la gouvernance de l'INPT à la gouvernance des SIC

Il n'existe pas de gouvernance des SIC des acteurs concourant aux missions de sécurité civile.

La mise en place de l'INPT offre l'opportunité de rapprocher des acteurs trop cloisonnés ou dispersés. En effet, les services utilisateurs vont devoir se partager les ressources de ce réseau. Ils vont donc se rencontrer, identifier et exprimer leurs besoins, expliquer voire clarifier leur organisation, rechercher des synergies et trouver des terrains d'entente.
Le futur OBNSIC[113] sera un des premiers référentiels partagés illustrant cette démarche.

Le comité de pilotage de l'INPT peut servir de « laboratoire » à un mode de gouvernance plus ambitieux. Son champ d'application pourrait rapidement s'élargir aux SIC suivant en cela, la logique d'interopérabilité des systèmes.

Dans le cadre d'une approche globale de la sécurité nationale (sécurité intérieure et sécurité civile) pourquoi ne pas imaginer une Direction Générale des SIC de Sécurité nationale sur le modèle de la Direction générale des SIC du ministère de la Défense[114] ? Tous les SIC seraient conçus et réalisés conformément à une politique générale garantissant, de ce fait, l'interopérabilité et la sécurité des systèmes. En matière de veille technologique et de recherche & développement, la cohérence et la complémentarité des projets seraient assurées.

---

[110] *Ibid*.
[111] *Ibid*.
[112] *Ibid*.
[113] Ordre de Base National des Systèmes d'Information et de Communication. Une 5ème version du projet vient d'être diffusée.
[114] Décret no 2006-497 du 2 mai 2006 portant création de la direction générale des systèmes d'information et de communication et fixant l'organisation du ministère de la défense en matière de systèmes d'information et de communication et arrêté du 6 juin 2006 portant organisation de la direction générale des systèmes d'information et de communication.

2.2 La construction du réseau

2.2.1 Des outils à forger

Une interopérabilité technique jugée insuffisante…

L'interopérabilité technique des moyens intervenant dans la gestion de crise est jugée insuffisante par le livre blanc de la Défense et de la Sécurité nationale[115].

Le contexte des nouveaux risques et menaces exige de développer l'interopérabilité des moyens intervenants dans la gestion de crise, « *en particulier les moyens d'information, de commandement et de communication des forces de sécurité publique, des forces de sécurité civile et des armées. La mise en place de liaisons fiables entre les différents acteurs conditionne en effet le déroulement de la gestion de la crise, en particulier dans les premières heures qui suivent son déclenchement*[116] ».

…et une maîtrise des NTIC à compléter

Ceci est surtout vrai pour les SDIS et les SAMU. En effet, police et gendarmerie disposent de services structurés et compétents[117] qui préparent et exécutent des programmes dans le cadre de stratégies élaborées par leur Direction Générale respective.

Les SAMU ne disposent pas de service dédié aux SIC. Leur expertise repose sur le service informatique de l'hôpital et l'investissement personnel de « bonnes volontés ». Pour leur SI, ils sont dépendants des programmes de modernisation décidés pour les hôpitaux, au niveau de l'ARS et du Ministère de la Santé.

Le manque d'homogénéité des SDIS se retrouve dans l'approche et les moyens que chacun peut consacrer aux TIC. Les plus avancés d'entre eux disposent des ressources et des compétences nécessaires au sein de groupements fonctionnels « SI ». Ils conduisent et réalisent des projets innovants à la pointe de la technologie[118]. Pour d'autres, le manque de temps et de moyens lié à la nécessité d'assurer au quotidien le maintien en fonctionnement des SI opérationnels et administratifs empêche toute prospective dans ce domaine. Ils sont équipés de produits « standard » fournis par des éditeurs spécialisés.

Un autre aspect est à prendre en considération. Les projets « SI » pèsent lourd sur l'organisation, en temps de réalisation comme en coût d'investissement. Mal maîtrisés, ils ont échaudé plus d'un décideur. Cependant, compte tenu du rôle de levier stratégique joué par les SI, le temps est sans doute venu pour les organisations les moins bien armées de se renforcer en compétences « réseaux ». A l'instar de ce qui s'est passé pour le contrôle de gestion avec le Directeur Administratif et Financier (DAF), la nécessité de maîtriser les NTIC pourrait se traduire par la généralisation d'un Directeur des Systèmes d'Information (DSI) au sein des équipes de direction.

Les acteurs de la sécurité civile les plus faibles doivent renforcer leurs compétences en TIC.

---

[115] Livre Blanc de la Défense et de la Sécurité nationale (2008 :194).
[116] *ibid*.
[117] La Sous Direction des Télécommunications et de l'Informatique à la DGGN et le Service des Technologies de la Sécurité Intérieure (STSI) à la DGPN.
[118] Je citerai de manière non exhaustive et pour exemples, les réalisations du SDIS 95 (Val d'Oise) et du SDIS 74 (Haute-Savoie) et les projets en cours du SDIS 64 (Pyrénées-Atlantiques), du SDIS 33 (Gironde), du SDIS 69 (Rhône) et du SDIS 01 (Ain).

Une stratégie européenne en R&D trop mal exploitée

L'Europe pour rattraper son retard - notamment sur les Etats-Unis - et assurer son indépendance géostratégique, mène une politique de recherche et développement (R&D) technologique basée sur des programmes-cadres pluriannuels.

Le septième programme-cadre, qui couvre la période 2007-2013, bénéficie d'un budget en augmentation[119] pour entraîner ainsi plus d'investissements nationaux et privés.

Il comporte un thème « Sécurité et espace »[120] dont les objectifs sont :

- développer les technologies et les connaissances axées sur des applications civiles afin de garantir la sécurité des citoyens face aux menaces (terrorismes, criminalité, catastrophes naturelles, accidents industriels, etc.) ;
- permettre une utilisation optimale et concertée des technologies disponibles et en cours de développement, à des fins de sécurité et dans le respect des droits fondamentaux de la personne humaine ;
- stimuler la coopération entre les fournisseurs et les utilisateurs de solutions en matière de sécurité ;
- renforcer la base technologique ainsi que la compétitivité de l'industrie européenne de la sécurité ;
- soutenir un programme spatial européen axé sur des applications telles que le système GMES[121], au bénéfice des citoyens et de la compétitivité de l'industrie spatiale européenne.

S'agissant de la sécurité, la priorité sera donnée à la dimension civile. La recherche sera multidisciplinaire. Dans les activités visées on trouve l'intégration et l'interopérabilité des systèmes.

Dans cette dynamique, organismes de recherche, industriels et acteurs de la sécurité civile s'investissent dans de nombreux projets R&D touchant à l'interopérabilité[122].

Sur ces projets, les acteurs de la sécurité civile sont trop dispersés. Il n'y a pas d'expression commune des besoins. Beaucoup de projets ne débouchent sur rien de concret faute d'approche globale.

De même, il n'existe pas de veille technologique commune des acteurs de la sécurité civile sur les développements des technologies pouvant constituer des réponses aux besoins opérationnels.

---

[119] 50 521 millions d'euros pour la période 2007-2013, soit en moyenne 7 217 millions d'euros par an. Ce qui représente plus d'une fois et demie le budget annuel du 6e programme-cadre,
http://europa.eu/legislation_summaries/energy/european_energy_policy/i23022_fr.htm

[120] Les budgets alloués à l'espace et à la sécurité s'élèvent respectivement à 1430 et 1400 millions d'euros, *http://europa.eu/legislation_summaries/research_innovation/general_framework/i23026_fr.htm*

[121] Le système GMES est un réseau de collecte et de diffusion d'informations concernant l'environnement et la sécurité basé sur la surveillance spatiale et in situ de la Terre. Ce système sera un appui à la prise de décision par les autorités publiques et privées en Europe, et un soutien à la recherche,
http://europa.eu/legislation_summaries/research_innovation/research_in_support_of_other_policies/l28170_fr.htm

[122] Citons le projet OASIS (Open Advanced System for dISaster and emergency management). Ce projet mené par la société EADS a débuté en 2004 pour s'achever en 2008. Il a porté sur l'élaboration d'un modèle interopérable d'échange de données au niveau opérationnel (format « ouvert » XML).

Interopérabilité et sécurité/confidentialité : un paradoxe à dépasser

Autres domaines qui méritent une approche globale : ceux de la sécurité des systèmes d'information et de la confidentialité de certaines données. En effet, ce sont des problématiques partagées par tous les acteurs.
Plus un système est ouvert, plus il est vulnérable en terme de sécurité. L'interopérabilité peut donc être perçu de prime abord comme antinomique de la sécurité des systèmes d'information.
Pour les SIC du ministère de l'intérieur, il revient à la Direction de la Planification de Sécurité Nationale la mission de définir leur politique de sécurité.
Les SIC des SDIS et des SAMU, quant à eux, sont régis selon les règles élaborées par leur responsable SIC.
Pour ce qui concerne la question de la sensibilité et de la confidentialité des données, elle renvoie à la nécessaire classification de celles-ci.
On distingue deux grandes catégories d'informations pour lesquelles la protection est recherchée : les informations qui concernent la défense nationale et la sûreté de l'état, dites classifiées de défense, et les informations sensibles qui obéissent à des règles différentes.
Certaines informations de police et de gendarmerie relèvent du secret de l'instruction judiciaire ou d'une classification « défense ».
Les données détenues par les SDIS ne sont pas classifiées alors que certaines sont sensibles[123].
Enfin, certaines données du SAMU sont soumises au secret médical.

Les problématiques de sécurité et de confidentialité des données sont parfois invoquées pour freiner voire faire obstacle à l'interopérabilité[124]. Cet argument ne doit pas être bloquant car, en ce domaine, les techniques et les savoir-faire évoluent.
La discussion des acteurs sur ces questions peut s'appuyer sur l'expertise de la toute récente Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)[125].

La normalisation : un levier pour l'interopérabilité

La définition des besoins et la normalisation des équipements sont les voies à suivre pour atteindre l'interopérabilité.
Comme nous l'avons vu, la normalisation peut être une stratégie de conquête économique pour développer des marchés et imposer des standards (interopérabilité partielle). Il faut donc veiller à ce que la normalisation permette une interopérabilité totale (connaissance intégrale des interfaces) pour créer un marché où les utilisateurs restent libres de leur choix et les industriels dans la capacité de développer et proposer des produits innovants.
Au niveau international, beaucoup de normes[126] sont édictées par des comités de normalisation[127] pour garantir l'interopérabilité. Concernant la gestion des crises, il est

[123] Par opposition aux informations classifiées qui reçoivent un label « officiel », sont qualifiées de sensibles :
les informations qui porteraient atteinte :
- au secret des délibérations du gouvernement,
- à la monnaie et au crédit public, à la sécurité publique,
- au secret de la vie privée, des dossiers personnels et médicaux,
- au secret en matière commerciale et industrielle,
- à la recherche, par les services compétents, des infractions fiscales et douanières ;
les informations qui restent soumises à l'obligation de réserve ou de discrétion professionnelle ;
les informations constitutives du patrimoine scientifique, industriel et technologique.
[124] Evoquons également ici, l'argument de la responsabilité qui pourrait être engagée en cas de partage d'une « mauvaise » information.
[125] Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ».
[126] Les normes ISO (International Standardization Organisation)..
[127] Exemple: le consortium OASIS (Organization for the Advancement of Structured Information Standards).

à noter qu'un comité technique[128] travaille à l'élaboration de normes internationales dans le domaine de la sécurité sociétale. Ces normes visent à « *accroître, chez toutes les parties intéressées, les capacités de continuité d'exploitation et de gestion de crise, par le biais d'améliorations en matière d'interopérabilité technique, humaine, organisationnelle et fonctionnelle ainsi que par une prise de conscience partagée des éléments contextuels*[129] ».

En France, dans le droit fil du programme ANTARES, la DSC a lancé un important travail réglementaire et normatif visant non seulement à développer l'interopérabilité mais aussi à la maîtriser.

- Les textes

Tout d'abord, l'article 9 de la loi de modernisation de la sécurité civile annonce un décret pour fixer « *les règles et normes techniques permettant d'assurer l'interopérabilité des réseaux de communication radioélectriques et des systèmes d'information des services publics qui concourent aux missions de sécurité civile* ».
Cet ensemble de règles et normes techniques prend l'appellation d'Architecture Unique des Transmissions (AUT)[130].
L'AUT s'applique aux réseaux de communications radioélectriques des principaux acteurs concourant aux missions de sécurité civile (moyens nationaux de la sécurité civile, SDIS, BSPP, BMPM, police et gendarmerie nationale, SAMU)[131]. Les équipements utilisés devront permettre d'exploiter l'INPT pour pouvoir être déclarés conformes à l'AUT[132].
Un projet d'arrêté relatif au règlement d'organisation nationale des SIC de sécurité civile est en préparation[133]. Ce document fixera les règles de mise en œuvre de l'AUT et les exigences de conformité aux normes et référentiels techniques pour l'ensemble des matériels, équipements, logiciels, applications, constitutifs des systèmes d'information.

- Le GT399

En association avec l'AFNOR, la DSC a lancé une démarche volontaire de certification animé par Infocert[134] : le GT399.
Le GT399 est un groupe de travail composé d'une quarantaine de membres actifs qui se réunit en moyenne tous les deux mois. Les membres sont des utilisateurs, tels que les médecins urgentistes, des représentants des SDIS ou du commandement des formations militaires de la sécurité civile (ComForMISC) et des fournisseurs comme SMANN TELECOM, SIS, ICOM France, ou SYSTEL. La FNSPF et Samu de France officient à la fois en tant qu'utilisateur et expert.
Conçu initialement pour accompagner les évolutions des règles de certification de la marque NF « Logiciel de sécurité civile » des équipements ANTARES, le GT 399 a, depuis la fin de l'année 2008, pris une orientation plus large visant à édicter les exigences AFNOR GT399 pour l'ensemble des outils et systèmes qui concourent aux missions de sécurité civile. Les exigences de qualité sont établies par concertation entre utilisateurs et fournisseurs.

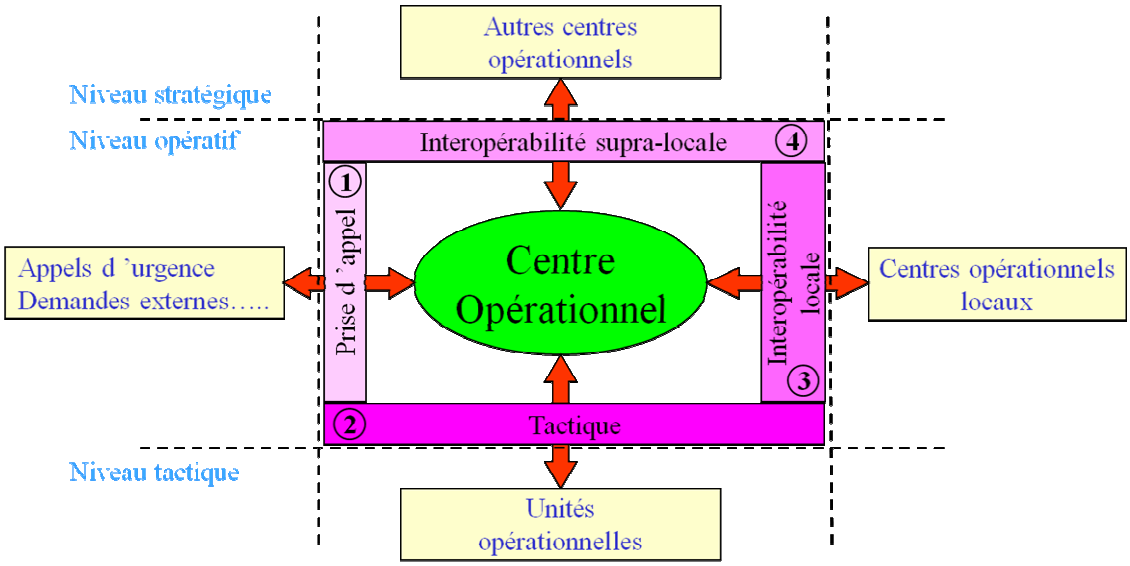
---

[128] Le Technical Comittee 223 ou TC223.
[129] Extrait du site ISO - Comité technique - TC223 - risque sociétal, *http://www.iso.org/iso/fr/iso_technical_committee.html?commid=295786*
[130] Article 1 du décret n° 2006-106 du 3 février 2006 relatif à l'interopérabilité des réseaux de communication radioélectriques des services publics qui concourent aux missions de sécurité civile.
[131] Article 2 du décret n° 2006-106.
[132] Article 3 du décret n° 2006-106.
[133] Cet arrêté (le futur OBNSIC) annulera et remplacera les dispositions de la circulaire NOR/INT/E/90//00219/C du 10 octobre 1990 relative à l'ordre de base national des transmissions de la sécurité civile.
[134] Organisme gestionnaire de la marque NF « logiciel de sécurité civile », Infocert assure le secrétariat technique du GT399.

Quatre sous-groupes (SGT) ont été constitués pour chaque flux d'informations qui ont été identifiés autour du centre opérationnel local (niveau départemental) :

- SGT1 : prise d'appel (appels d'urgence ou flux entrants, acquisitions d'informations) ;
- SGT2 : tactique (flux avec les moyens sur le terrain) ;
- SGT3 : interconnexion des centres opérationnels locaux (interopérabilité locale, flux entre CTA/CODIS– CTA/CODIS, CTA-CRRA, etc.) ;
- SGT4 : interconnexion des centres opérationnels nationaux (interopérabilité supra locale, flux entre centres opérationnels locaux et centres opérationnels régionaux, nationaux).

Le schéma suivant illustre et résume la démarche :



Source : direction du programme ANTARES, SDSPAS, DSC

A partir des besoins exprimés par les utilisateurs, l'objectif est le développement d'applications et d'outils répondant à ces besoins tout en ne bridant pas l'imagination des industriels.
Le GT399 a déjà produit des résultats concrets dans le domaine des secours et des soins d'urgence (exploitation de la voie « data » du réseau ANTARES pour les bilans secouristes, médicaux, ECG…)[135] et dans le domaine de la rénovation du RNA (remplacé par le SAIP).
La certification NF399 va garantir, dans un premier temps, la cohérence et l'interopérabilité des projets de modernisation et d'interconnexion des SIC des SDIS et des SAMU, avant de s'étendre à l'ensemble des SIC de sécurité civile.

La normalisation est un processus long et coûteux[136] mais l'enjeu d'interopérabilité qu'il porte justifie un engagement fort de l'Etat pour « écrire la règle ». Le GT399 joue un rôle moteur essentiel dans le développement de l'interopérabilité. Il a vocation à être étendu à tous les acteurs concourant aux missions de sécurité civile.

[135] Le référentiel d'interopérabilité faisant référence aux formats de données des bilans médical et secouriste doit être publié en fin d'année.
[136] Les frais d'inscription au GT399 s'élèvent, pour les fournisseurs, à 5.000 euros hors taxe la première année. Le renouvellement de la participation se chiffre ensuite à 2.500 euros hors taxe. La participation d'un utilisateur est gratuite.

2.2.2 Des matériaux à assembler

Savoir-faire et compétences

Les composantes principales concourant à la sécurité civile (moyens de l'Etat, pompiers, SAMU, police, gendarmerie, …) possèdent des compétences et des savoir-faire éprouvés et reconnus, voire enviés par les autres pays.
Leurs structures et leurs managements sont dynamiques et s'appuient sur des référentiels en évolution permanente.
Chaque « partenaire » possède des « cœurs de métier » lui permettant d'être chef de file dans des projets d'interopérabilité.

Les conditions sont donc remplies pour élaborer un référentiel de sécurité civile. Véritable lexique ou dictionnaire interservices, cette interopérabilité de doctrine et de procédures est un préalable à l'interopérabilité matérielle.

La stratégie « réseaux » de la Gendarmerie Nationale

La gendarmerie a été la première à mettre en œuvre, dès les années 80, une stratégie d'équipement de réseaux, qui répond à ses besoins et qui s'appuie sur les NTIC (SAPHIR, RUBIS).
En 2000-2002, elle fait le constat suivant :

- Les systèmes sont peu souples et très dépendants de certains éditeurs. Ils sont très coûteux sur le long terme et ils sont peu interopérables ;
- Le contexte pousse à une plus grande rationalisation et à une réorganisation (renforcement des zones périurbaines entraînant le regroupement des unités rurales) ;
- Le réseau IP (Intranet) est trop peu déployé (200 sites sur 4000).

A partir de ce constat, la gendarmerie change de stratégie[137]et mise sur le « tout normalisé » et l'indépendance vis-à-vis des éditeurs.
Les objectifs fixés sont :

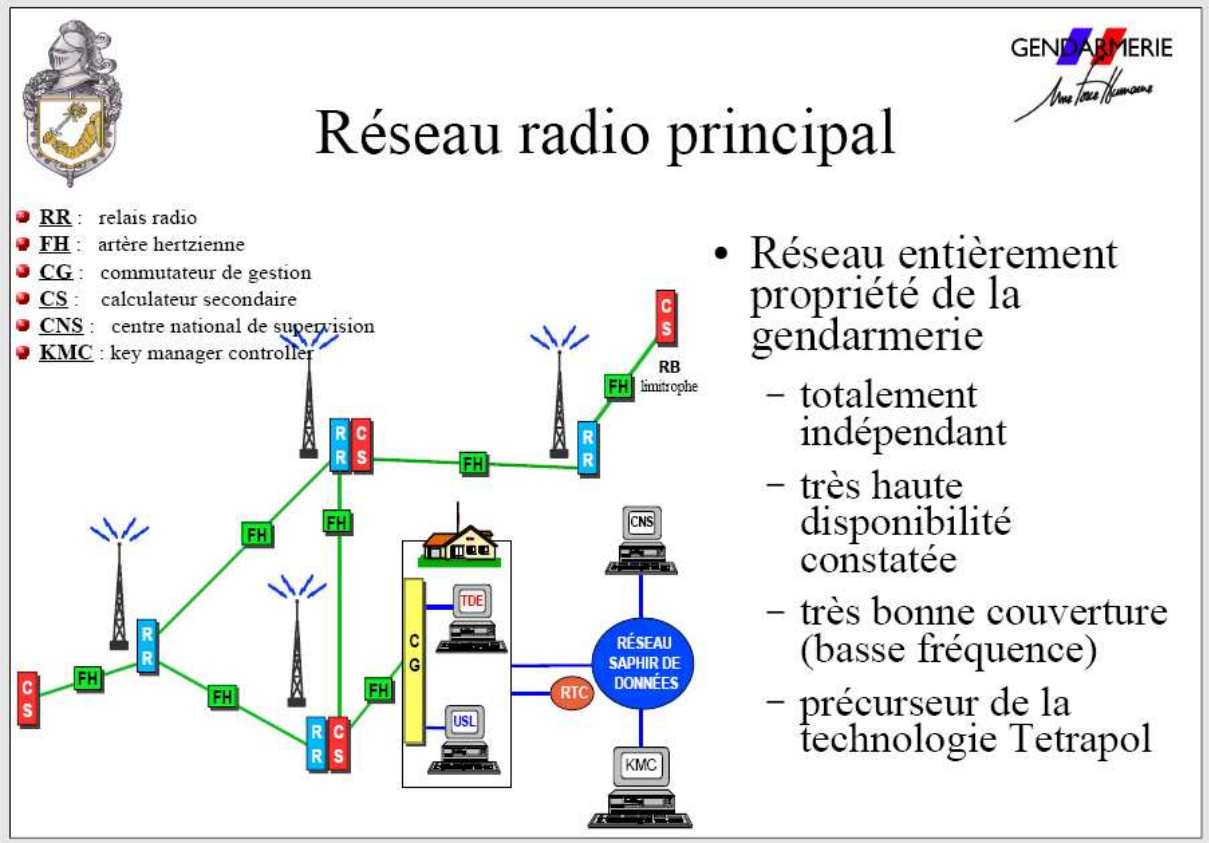
- un SIC moderne au service de la performance ;
- une capacité d'interopérabilité ;
- une maintenance rationalisée ;
- une sécurité, une performance et une fiabilité optimales.

Pour les atteindre, la gendarmerie garde la maîtrise du socle technique (maintenance) et fait le choix d'un système modulaire dont les modules dialoguent entre eux uniquement par des protocoles ouverts et libres de droits. Quand elle externalise des applications « métiers », elle oblige le fournisseur à un transfert de compétences pour pouvoir confier le support à un autre industriel au renouvellement du marché.
Enfin, elle fait le choix de l' « open source » pour les applications bureautique (open office), la messagerie (Firefox et Thunderbird) et le système d'exploitation (Linux/Ubuntu).

La gendarmerie dispose au final, d'un réseau cohérent, adapté à ses besoins, résilient[138], économique et sûr. Elle en est l'opérateur et le propriétaire.

---

[137] *La politique des logiciels de la gendarmerie nationale, Sous – Direction des Télécommunications er de l'Informatique – bureau de la sécurité et de l'architecture - Lieutenant colonel Xavier Guimard.*



Source : Gendarmerie Nationale

En 2005, la gendarmerie considère que les transmissions relèvent de l'opérationnel et non du « soutien », et qu'à ce titre, elles font partie intégrante de son « cœur de métier ».
Elle met en œuvre une stratégie de renforcement de son réseau.
RUBIS passe sur technologie IP et SAPHIR évolue vers un Intranet sécurisé déployé sur 4300 sites à travers le monde.
L'opération sur SAPHIR 3G est attribuée à la société Orange Business Service (OBS). Cependant, la gendarmerie garde le contrôle sur un «backbone[139] » tactique de 200 sites qu'elle considère comme vital.

Aujourd'hui, la gendarmerie va faire évoluer RUBIS[140] pour qu'il permette la transmission « voix + data » à un débit de 8Mbit/s. Ce débit « natif » pourra augmenter en fonction de l'évolution des besoins.

Les réseaux ACROPOL/ANTARES et RUBIS arriveront en « fin de vie » en 2020. A cette date, la gendarmerie parie sur une technologie[141] qui permettra de mixer son réseau 80MHz avec le réseau 400MHz ACROPOL/ANTARES.

Le résultat sera l'INPT « complète » ou « INPT2 ».

Dans les domaines des réseaux, la gendarmerie possède une expérience et une expertise qu'elle peut partager avec les autres acteurs concourant aux missions de sécurité civile.

---

[138] Toute l'infrastructure de communication est à base de faisceaux hertziens. Cette infrastructure a résisté aux vents violents de la tempête KLAUS.
[139] Colonne vertébrale.
[140] Un marché est prévu sur 2010-2013.
[141] Une passerelle 80-400MHz ou la « radio numérique logicielle », une technologie révolutionnaire qui permettrait de créer par un logiciel la fréquence désirée. Les sociétés EADS et THALES y travailleraient.

L'interopérabilité de doctrines des SDIS

Schéma Départemental d'Analyse et de Couverture des Risques, centralisation du 18, système informatisé de gestion opérationnelle, Référentiel Emplois-Formation, Guides Nationaux de Référence, normes de matériels, textes réglementaires, incitations financières …

Piloté par l'Etat et les élus locaux, associant SDIS et consultants indépendants, la méthode employée pour la « départementalisation » des SDIS a permis en moins d'une décennie[142] d'unifier la doctrine opérationnelle.
Les anciens corps communaux sont devenus les centres d'incendie et de secours du corps départemental. Dans une démarche très proche de la démarche capacitaire[143], les SDIS démontrent aujourd'hui leur aptitude à mobiliser et à projeter leurs moyens dans et hors du département.
Constitués à partir de briques autonomes (les groupes) identifiées par domaine d'emploi opérationnel (incendie, secours à personnes, inondation, feux de forêt, énergie, etc.), ces moyens peuvent se combiner pour former des ensembles (les colonnes) interopérables avec les moyens du ou des SDIS de la zone sinistrée.
Les constitutions à titre préventif des colonnes de renfort « feux de forêt » et la gestion récente de la crise de l'ouragan « Klaus » illustrent cette aptitude.

Ce qui a été réalisé lors du processus de départementalisation des SDIS peut servir de modèle en matière d'interopérabilité des doctrines.

Les images de la Police Nationale

Le développement de l'utilisation de la vidéoprotection est un des objectifs des lois d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI). Le pôle « mobilité » de la Division des programmes opérationnels de la Police Nationale expérimente avec les opérateurs France Telecom et SFR des solutions hauts débits permettant la transmission d'images vidéo.
L'idée est d'équiper les véhicules de police de caméra dont les images sont stockées sur disque dur, ceci à des fins de vidéoprotection. Quand un véhicule intervient sur une agression ou tout autre acte délictueux, il transmet les images prises par sa caméra aux autres véhicules arrivant en renfort ainsi qu'au CIC. Ce système permet une anticipation et accroît la sécurité des équipages.

Dans l'exploitation des images de vidéoprotection, la police possède une expertise qui intéresse les autres acteurs concourant aux missions de sécurité civile.

Des outils et des besoins communs

Il n'y a pas d'approche globale dans la conception des SIC et pourtant les outils et leurs fonctionnalités ne sont pas si éloignés.

SAMU, Gendarmerie, Police, Pompiers, ces 4 services disposent :

- d'un centre équipé d'un système de réception et de traitement des appels d'urgence,
- d'un centre opérationnel équipé d'un système de gestion opérationnelle permettant de suivre l'opération et de la tracer, de communiquer avec les

[142] La loi n°96-369 du 3 mai 1996, dite de « départementalisation » fixait un délai de 5 ans.
[143] Issue du domaine militaire, la démarche capacitaire est un processus d'élaboration d'une capacité de forces qui s'appuie sur 5 piliers : la doctrine – les équipements – les ressources humaines – l'entraînement et les exercices - le soutien.

moyens engagés, d'exploiter des bases de données pour le soutien aux opérations (cartographie enrichie de données « métiers », table de matières dangereuses, procédures, etc.),
- d'un certains nombres d'outils de communication et de messagerie pour l'échange d'information.

Aujourd'hui, les TIC permettent d'exploiter les flux vidéo et cartographiques et peuvent intégrer les interfaces de communication au sein des systèmes de gestion opérationnelle.

Aussi, SAMU, Gendarmerie, Police et Pompiers expriment-ils des besoins très proches :

- disposer de capteurs et de terminaux embarqués équipant leurs équipes sur le terrain pour échanger avec le SIC du centre opérationnel (images, visualisation des scènes, données, géolocalisation…),
- coupler au système de gestion opérationnelle un SIG. Enrichir le SIG en données « métier » par la collecte ou la récupération de bases de données géoréférencées,
- interconnecter leur SIC sur les réseaux pour échanger avec leurs centres opérationnels, exploiter l'information des systèmes de veille et de surveillance déployés sur le terrain (caméras, détection de départs de feux, …),
- intégrer les messageries « opérationnelles » (portail ORSEC) dans le SIC pour éviter les doubles saisies,
- intégrer les outils statistiques et les fonctionnalités de tableaux de bord dans le SIC.

La convergence des SIC au niveau départemental

La police nationale et la gendarmerie nationale lancent des marchés pour rénover leurs centres opérationnels.

Pour la police, il s'agit du projet MCIC 2 de modernisation de leurs Centre d'Information et de Commandement autour du système PEGASE[144]. Le marché attribué en 2009 comporte une phase initiale d'étude et de développement puis un déploiement qui devrait débuter en 2012. Tous les CIC des départements sont concernés ainsi que les centres de la police de l'air et des frontières (PAF) et des CRS, soit 122 sites.

La gendarmerie a attribué un marché en 2008 pour le projet ATHEN@[145]. Il s'agit d'un SIC qui va relier l'ensemble des brigades, des Centres d'Opérations et de Renseignement de la Gendarmerie (CORG) , les centres régionaux et nationaux, soit 4000 sites. Le déploiement débute en 2010.

Les fonctionnalités de PEGASE et d'ATHEN@ répondent aux besoins que nous avons mis en exergue, (cartographie, flux vidéos, géolocalisation, messagerie intégrée…).

Les SAMU modernisent également leur SI dans le cadre de démarches de mutualisations. Ainsi l'Assistance Publique des Hôpitaux de Paris (APHP) dote tous les établissements hospitaliers de Paris et de la petite couronne d'un SI global, intégré et interfacé[146]. Le système sera interopérable et redondant.

[144] Pilotage des Evénements et Gestion des Activités et des Equipages.
[145] Application de gestion des opérations et du traitement des informations d'ordre public et de défense.Le marché a été attribué aux sociétés THALES et TECHWAN.
[146] Système CARMEN. Les Hauts-de-Seine (92) est le premier département équipé fin 2009. Ensuite suivront Paris (75), la Seine St Denis (93) et le Val-de-Marne (94).

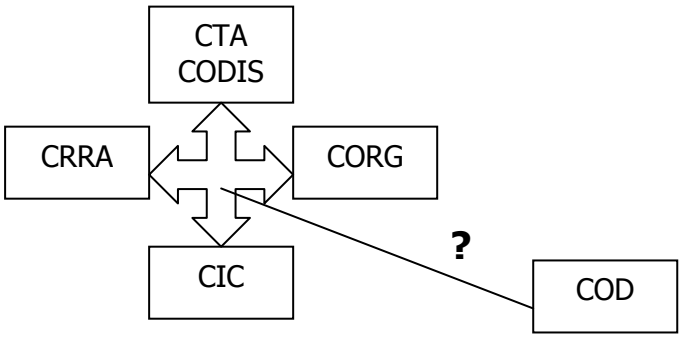
Cependant cette situation ne reflète pas une réalité générale. Les SAMU sont hétérogènes en matière de SIC.

Nous assistons à un mouvement de convergence des fonctionnalités des SIC. En les interconnectant, il devient possible de partager les informations d'un certain nombre de données de références : nature de l'intervention, adresse, moyens engagés, géolocalisation, information géographique, images vidéos, événements « portail ORSEC », etc.

Au niveau départemental, un scénario d'interconnexion en deux étapes peut s'envisager :

- 1ère étape : interconnexion SDIS-SAMU et CIC-CORG (2010-2020)

- 2ème étape : interconnexion SDIS-SAMU-CIC-CORG (à partir de 2020)



Une liaison vers le COD permettrait au DOS (une fois le COD activé) de conduire la crise en disposant de toutes les informations nécessaires. On retrouverait au COD, des postes interfaces reliés aux SIC des centres opérationnels locaux pour « construire » une image consolidée de la situation opérationnelle.

Cependant, comment garantir l'efficacité d'une structure qui n'est activé qu'en situation de crise ? Les outils de gestion de crise pour qu'ils fonctionnent le jour J doivent être des outils utilisés au quotidien par des personnels formés et entraînés.

Aménager les CODIS, les CIC et les CORG pour qu'ils puissent tenir le rôle du COD dans les premiers instants de la crise est pragmatique et correspond à la réalité du fonctionnement quotidien de la sécurité civile au niveau local.

Un cadre incitatif à mettre en place

Actuellement aucun dispositif incitatif n'existe visant à favoriser l'interconnexion et l'interopérabilité des SIC des principaux acteurs concourant aux missions de sécurité civile.

Ce qui est fait dans le cadre du programme ANTARES peut être étendu : attribution de part du FAI (aide financière), obligation dans le cadre du renouvellement d'équipement (textes réglementaires), référentiels techniques (groupe de normalisation), référentiels de doctrine (exemple du référentiel SAP/AMU), communication sur les « plus-values » (géolocalisation, sécurité des intervenants, …).

L'argument financier plaide en faveur de la mutualisation des SIC et/ou de leur interconnexion.

Le regroupement des centres de réception des appels

La tendance de nos voisins européens est de regrouper les centres de réception des appels à l'occasion de leur modernisation.

Cette mutualisation s'opère selon deux axes qui peuvent se combiner :

- un regroupement des numéros d'urgence qui équivaut à la mise en place du 112, numéro unique européen pour l'urgence (exemple de la Finlande) ;
- un regroupement des centres de réception locaux en quelques centres régionaux (Angleterre, Espagne), voire en un seul centre national (Finlande).

Le regroupement en un même lieu rationalise les infrastructures, les équipements et optimise la gestion des opérateurs.

Le Secrétariat Général du Ministère de l'Intérieur étudie la faisabilité d'un regroupement dans un centre régional, des centres de réception du 17 qui se trouvent actuellement au niveau départemental.

Certains SDIS[147] étudient la possibilité d'interconnecter leur CTA-CODIS pour pouvoir se « secourir » en cas de saturation d'appels.

Si le regroupement, du niveau local au niveau régional, des centres de réception et de traitement des appels d'urgence peut être envisagée, cette possibilité semble exclue pour les centres opérationnels locaux.
En effet, le principe d'organisation du commandement unique du Maire (commune) ou du préfet (département) impose de conserver les centres de conduite opérationnelle à ce niveau.

Sous cette condition, il peut être envisagé de les regrouper en un même lieu.

[147] Les SDIS 01 (Ain) et 69 (Rhône) testent actuellement l'interconnexion des SIC de leurs CODIS respectifs. Cette interconnexion peut permettre la « supervision » des moyens défendant les zones limitrophes des départements et autoriser le département X à déclencher directement les moyens du département Y qui défend une commune du département X.

Le regroupement des centres opérationnels locaux

Au niveau départemental, le regroupement des centres opérationnels peut se concevoir selon trois types de plates-formes dont les avantages/inconvénients sont résumés dans le tableau suivant :

<table>
<tr><th>Type de plate-forme</th><th>AVANTAGES</th><th>INCONVENIENTS</th><th>Observations</th></tr>
<tr><td>Plate-forme commune « physique » avec SIC différents</td><td>Economie d'échelle par mutualisation d'infra, d'équipements.

Interconnexion et interopérabilité partielle des SIC garantie par le respect de normes techniques.</td><td rowspan="2">Nécessite une « synchronisation » de tous les acteurs dans leur besoin de renouvellement d'infrastructures.

Nécessite un important travail en commun pour l'élaboration du cahier des charges.

Investissement lourd au départ.

Nécessite une sécurisation par redondance qui peut être lourde.</td><td rowspan="2">Semble difficilement réalisable car Police et Gendarmerie s'engagent chacun de leur côté dans des programmes de modernisation de leurs centres opérationnels.

Des plates-formes de ce type existent et fonctionnent entre SDIS et SAMU.</td></tr>
<tr><td>Idem mais avec SIC unique</td><td>Economie d'échelle par mutualisation d'infra, d'équipements.

Interconnexion et interopérabilité totale garantie.

Mutualisation des personnels possibles (opérateurs).</td></tr>
<tr><td>Plate-forme commune « virtuelle » avec des SIC différents</td><td>Interconnexion et interopérabilité partielle des SIC garantie par le respect de normes techniques.

Ne nécessite pas la « synchronisation » de tous les acteurs dans leur besoin de renouvellement d'infrastructure.

Solution « souple » permettant d'inclure police et gendarmerie et d'autres acteurs « à la carte ».

Chacun reste « chez soi », dans son environnement.</td><td>Difficultés liés à la volonté d'échanger des acteurs.

L'interopérabilité totale n'est pas garantie (« contraintes » d'éditeurs).

Pas d'économie d'échelle par mutualisation (sauf à s'équiper du même SIC). Dépense qui peut être ressentie comme non indispensable.</td><td>Des plates-formes de ce type existent et fonctionnent entre SDIS et SAMU.

Elles devraient se multiplier sous l'impulsion du référentiel SAP/AMU.</td></tr>
</table>

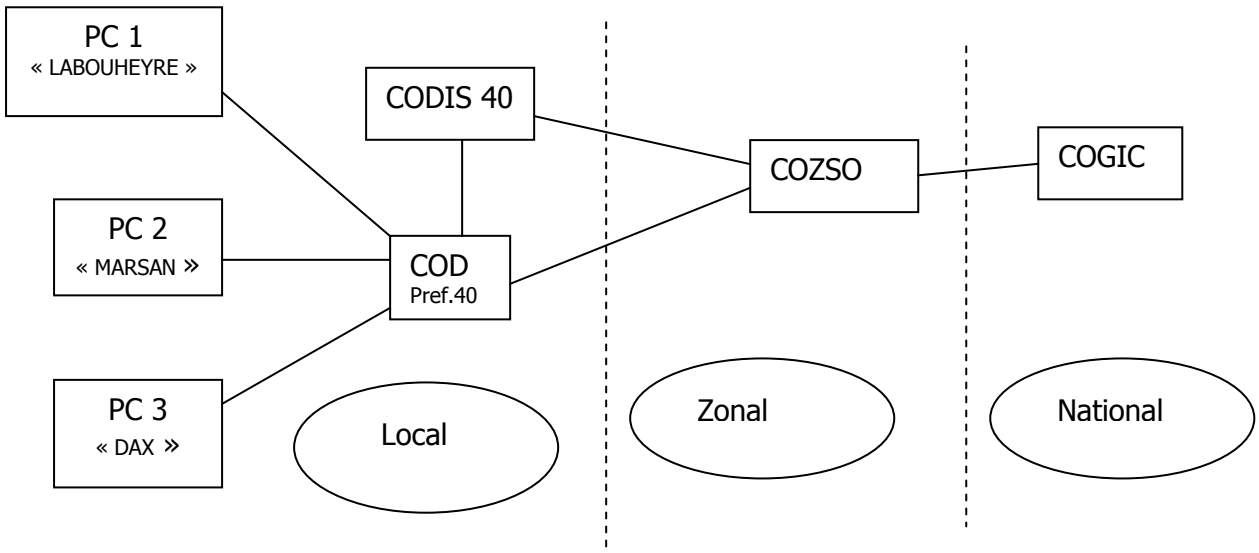
La solution d'une plate-forme commune « physique » s'avère plus coûteuse au départ mais elle est intéressante à long terme si tous les acteurs sont dans une dynamique de renouvellement de leurs plateaux techniques.
Sinon, la solution d'une plate-forme « virtuelle » est plus souple et plus économique.

La chaîne de commandement de la sécurité civile : lignes de forces de l'interopérabilité

En situation de crise, la répartition des rôles dans l'organisation actuelle peut se résumer comme suit :

- Commandement et Action au niveau local (départemental),
- Evaluation et Soutien au niveau zonal et national.

La chaîne de commandement mise en place par les sapeurs pompiers et la Sécurité Civile a fait ses preuves et a démontré toute sa cohérence et son efficacité dans la gestion de crise. Nous pouvons l'illustrer telle qu'elle a fonctionnée pour la gestion de l'ouragan KLAUS :



Le développement de l'interopérabilité et l'interconnexion des SIC doivent être architecturés le long de ces lignes guides, véritables lignes de force de l'organisation de crise de la sécurité civile.

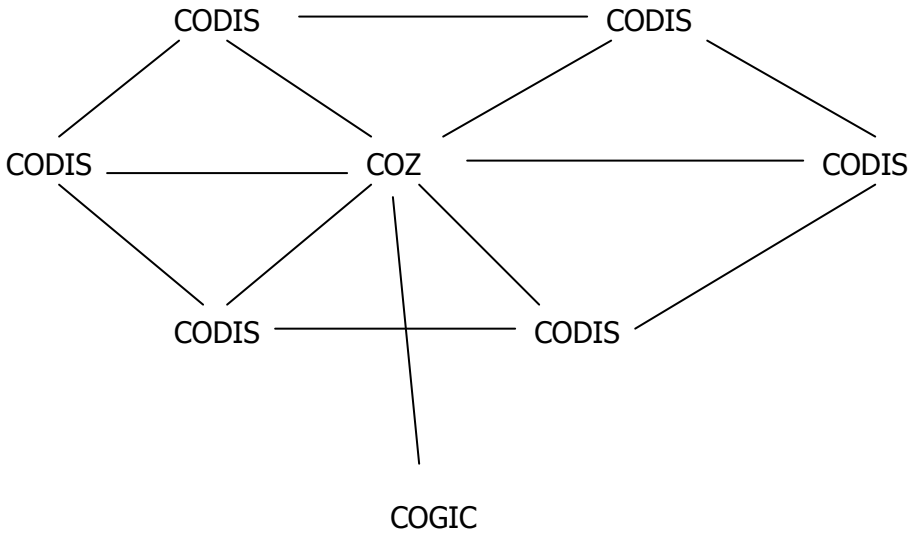
Une expérimentation des communications à partir de liaisons satellites sur la chaîne PCO-{COD-CODIS}-COZ-COGIC est menée actuellement dans la Zone de Défense Sud-Est par la DSC (direction du programme ANTARES), le COZ Sud-Est et les SDIS 69 (Rhône) et 01 (Ain). Le PC de site « pompiers » est équipé d'un module satellite pour fournir sur la zone d'intervention une « bulle » de communications à tous les services impliqués dans les opérations.

Pour la gestion de crise, le préfet, Directeur des opérations de secours (DOS) confie, en règle générale, la fonction de Commandant des opérations de secours (COS) au DDSIS. Il revient à ce dernier de coordonner l'action de tous les services.
Les SDIS ont donc développé des compétences et des équipements en matière de coordination opérationnelle. Leurs PC de site deviennent les PC de coordination interservices (PCO) et les CODIS activés 24/24 centralisent les informations dès le début de la crise.

Vers un réseau zonal

Un Intranet sécurisé, pourrait relier entre eux les différents SIC des CODIS, tous certifiés NF399.
Les SIC intégreraient « nativement » l'application « portail ORSEC ». Ils alimenteraient un entrepôt de données zonal permettant aux COZ de réaliser une veille sur les « signaux faibles » de l'activité opérationnelle remontant en temps réel sur des « tableaux de bord ».
De part ses fonctions d'anticipation, de préparation, de soutien et d'évaluation, le SIC du COZ renseignerait également des indicateurs consultables par les CODIS.
La connexion en réseau de ces entrepôts de données sur le modèle des RCC anglais permettrait une sécurisation par redondance et une centralisation de l'information au niveau national.

L'ensemble dessine une architecture des centres opérationnels.

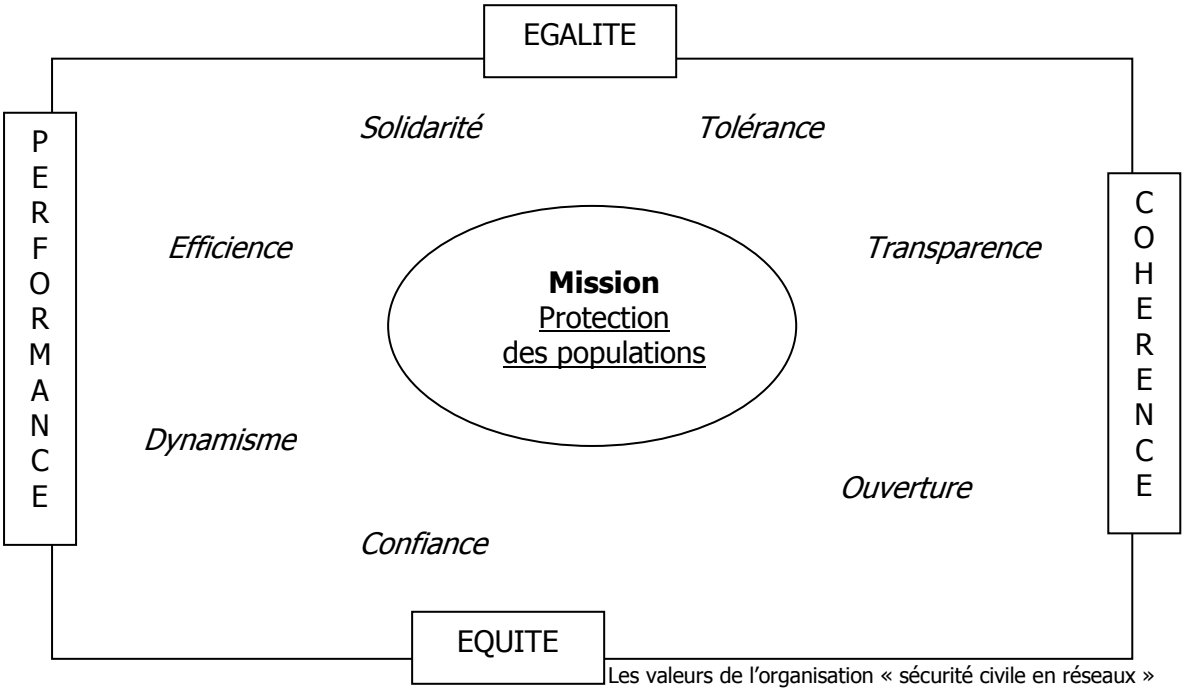


3 PLAN D'ACTION STRATEGIQUE (2010-2020)

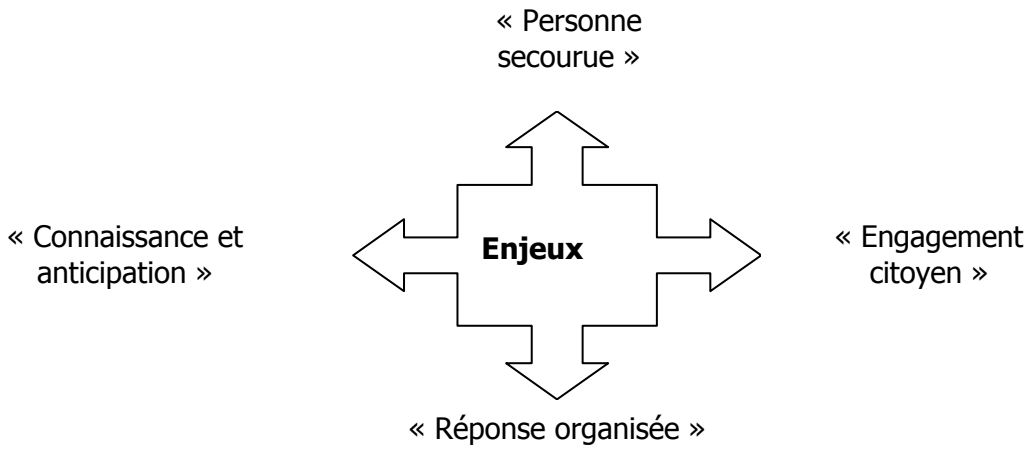
Vision

Une Sécurité Civile globale, en réseau d'acteurs qui unissent leurs forces pour une réponse coordonnée, efficace et efficiente, à la hauteur des risques et menaces de notre temps.

Schéma des valeurs du réseau « sécurité civile »



Les valeurs de l'organisation « sécurité civile en réseaux »



4 Orientations Stratégiques (OS)

Mettre en place une gouvernance des SIC

Réaliser un référentiel d'interopérabilité

Maîtriser les NTIC

Développer une culture de l'interopérabilité

26 Recommandations (R)

R1 - Faire de la gouvernance de l'INPT le « laboratoire » de la gouvernance des SIC
R2 - Elaborer une charte managériale entre les acteurs
R3 - Réfléchir à une nouvelle gouvernance des acteurs
R4 - Réfléchir à l'architecture du SIC de l'organisation « sécurité civile »
R5 - Créer au niveau national, une instance interministérielle de gouvernance des SIC des acteurs concourant aux missions de sécurité civile et associant également les Collectivités Territoriales et les secteurs d'activités d'importance vitale
R6 - Utiliser nos savoirs pour élaborer des standards et développer des référentiels communs
R7 - Faire de la normalisation le levier de l'interopérabilité
R8 - Inventorier les données et les SI détenus par chacun - Identifier les données « coeur de métier » de chacun - Identifier les besoins de chacun - En déduire les échanges et les partenariats à mettre en place
R9 - Réfléchir à la « standardisation » des centres de réception/traitement des appels et des centres opérationnels, à leur interconnexion « native », à leur maillage autour d'entrepôts de données
R10 - Participer à la déclinaison de la directive INSPIRE en adhérant aux projets de mutualisation de l'information géographique et réaliser un catalogue de données « sécurité civile »
R11 - Assurer une veille stratégique dans le domaine des NTIC répondant aux besoins exprimés par les utilisateurs
R12 - Répondre aux appels à projets en R&D touchant à l'interopérabilité
R13 - Intégrer les problématiques de SSI et de confidentialité des données
R14 - Réfléchir à l'adaptation des outils TIC
R15 - Diminuer les risques inhérents aux NTIC en renforçant les structures en « spécialistes réseaux»
R16 - Passer des partenariats avec les services « experts » (Défense, MEEDDM, industriels, organismes de recherche, universités, etc.)
R17 - Concevoir et/ou redéfinir les « tuyaux » nécessaires à l'interopérabilité
R18 - Développer l'interopérabilité dans le cadre de la RGPP
R19 - Lancer en priorité les projets d'interopérabilité sur les besoins communs des acteurs (information géographique, vidéo, géolocalisation)
R20 - Relier les centres opérationnels en commençant par le « cœur » de l'organisation de sécurité civile : liens CODIS-CODIS, PCO-CODIS-COD-COZ-COGIC
R21 - Concevoir un SI intégré « conduite de crise » au bénéfice du DOS
R22 - Tirer des enseignements en termes d'interopérabilité, à partir des entraînements organisés avec tous les acteurs sur les scénarios mettant en jeu les nouveaux risques et menaces
R23 - Faire émerger un réseau « sécurité civile » au sein des réseaux de l'Etat
R24 - Mettre en place un cadre incitatif pour les projets développant l'interopérabilité
R25 - Sensibiliser les acteurs et les décideurs à l'interopérabilité
R26 - Faire de l'INPT le vecteur de l'interopérabilité

OS1

Mettre en place une gouvernance des SIC	
R1	Faire de la gouvernance de l'INPT le « laboratoire » de la gouvernance des SIC
R2	Elaborer une charte managériale entre les acteurs
R3	Réfléchir à une nouvelle gouvernance des acteurs
R4	Réfléchir à l'architecture du SIC de sécurité civile
R5	Créer au niveau national, une instance interministérielle de gouvernance des SIC des acteurs concourant aux missions de sécurité civile et associant également les Collectivités Territoriales et secteurs d'activités d'importance vitale

OS2

Réaliser un référentiel d'interopérabilité	
R6	Utiliser nos savoirs pour élaborer des standards et développer des référentiels communs
R7	Faire de la normalisation le levier de l'interopérabilité
R8	Inventorier les données et les SI détenus par chacun - Identifier les données « coeur de métier » de chacun - Identifier les besoins de chacun - En déduire les échanges et les partenariats à mettre en place
R9	Réfléchir à une « standardisation » des centres de réception/traitement des appels et des centres opérationnels, à leur interconnexion « native », à leur maillage autour d'entrepôts de données
R10	Participer à la déclinaison de la directive INSPIRE en adhérant aux projets de mutualisation de l'information géographique et réaliser un catalogue de données « sécurité civile »

OS3

Maîtriser les NTIC	
R11	Assurer une veille stratégique dans le domaine des NTIC répondant aux besoins exprimés par les utilisateurs
R12	Répondre aux appels à projets en R&D touchant à l'interopérabilité
R13	Intégrer les problématiques de SSI et de confidentialité des données
R14	Réfléchir à l'adaptation des outils TIC
R15	Diminuer les risques inhérents aux NTIC en renforçant les structures en « spécialistes réseaux »
R16	Passer des partenariats avec les services « experts » (Défense, MEEDDM, industriels, organismes de recherche, universités, etc.)
R17	Concevoir et/ou redéfinir les « tuyaux » nécessaires à l'interopérabilité

OS4

Développer une culture de l'interopérabilité	
R18	Développer l'interopérabilité dans le cadre de la RGPP
R19	Lancer en priorité les projets d'interopérabilité sur les besoins communs des acteurs (information géographique, vidéo, géolocalisation)
R20	Relier les centres opérationnels en commençant par le « cœur » de l'organisation de sécurité civile : liens CODIS-CODIS, PCO-CODIS-COD-COZ-COGIC
R21	Concevoir un SI « conduite de crise » au bénéfice du DOS
R22	Tirer des enseignements en termes d'interopérabilité, à partir des entraînements organisés avec tous les acteurs sur les scénarios mettant en jeu les nouveaux risques et menaces
R23	Faire émerger un réseau « sécurité civile » au sein des réseaux de l'Etat
R24	Mettre en place un cadre incitatif pour les projets développant l'interopérabilité
R25	Sensibiliser les acteurs et les décideurs à l'interopérabilité
R26	Faire de l'INPT le vecteur de l'interopérabilité

Les 6 « Quick wins »[148]

R2 : élaborer une charte managériale entre les acteurs

R6 : utiliser nos savoirs pour élaborer des standards et développer des référentiels communs

R10 : participer à la déclinaison de la directive INSPIRE en adhérant aux projets de mutualisation de l'information géographique et réaliser un catalogue de données « sécurité civile »

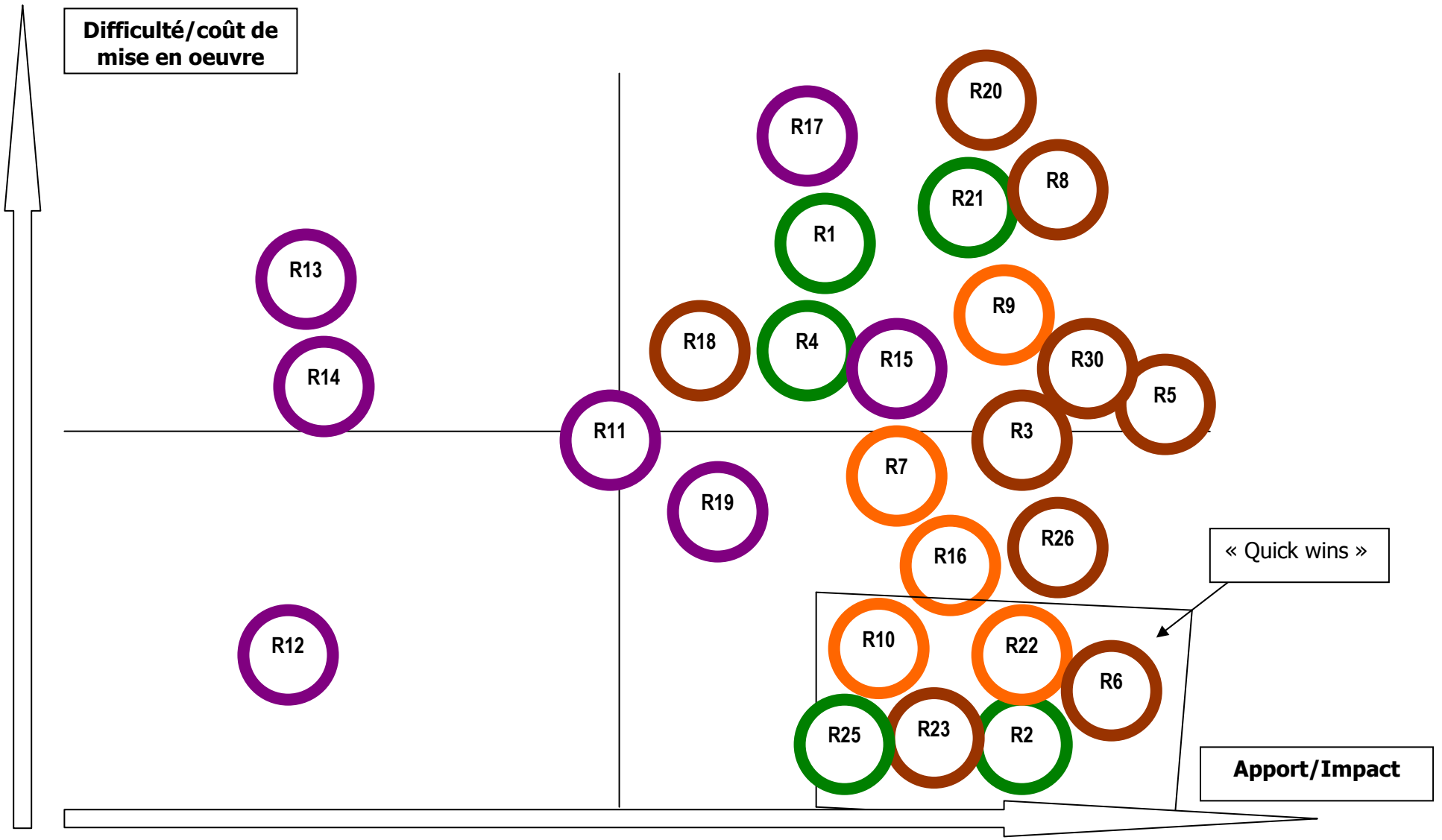
R22 : tirer des enseignements en termes d'interopérabilité, à partir des entraînements organisés avec tous les acteurs sur des scénarios mettant en jeu les nouveaux risques et menaces

R23 : faire émerger un réseau « sécurité civile » au sein des réseaux de l'Etat

R25 : sensibiliser les acteurs et les décideurs à l'interopérabilité

[148] Une matrice d'efficience sert à classer les recommandations selon leur impact et leur facilité de mise en œuvre. Les recommandations identifiées comme faciles à mettre en œuvre avec un impact fort (« quick wins ») sont des recommandations à mettre en œuvre immédiatement.

Matrice d'efficience



CONCLUSION

Maîtriser l'information est un enjeu stratégique majeur.

Demain, grâce aux outils des nouvelles technologies de l'information et de la communication, grâce aux réseaux et à l'interopérabilité des systèmes, le directeur « connecté » des opérations de secours bénéficiera d'une « chaîne d'informations » orientées pour la prise de décision en situation de crise.

Cependant, environnés par les outils « Hi Tech », habitués à agir avec toute la puissance des traitements informatiques, que ferons-nous en cas de panne ou de dérèglements de ces systèmes ? Des événements tels que la tempête KLAUS, sont là pour nous rappeler combien nous sommes dépendants de ces systèmes et combien ils sont vulnérables.

Aussi, l'Architecture Unifiée des Transmissions doit-elle garantir aux acteurs de la sécurité civile, une INPT sûre et sécurisée.

En 2020, augmentée des réseaux RUBIS et SAPHIR, l'INPT évolue pour devenir l'INPT2. Parallèlement, le déploiement achevé de l'infrastructure nationale de l'information géographique permet la numérisation de l'espace opérationnel. L'interopérabilité des systèmes trouve sa consécration dans l'exploitation par des postes de commandement multiservices, d'images consolidées de la situation opérationnelle.

Cette projection à 10 ans est conditionnée par les réponses à un certain nombre de questions en suspens. Quel(s) opérateur(s) pour l'INPT ? Quelle gouvernance ? Quelle sera l'évolution des SDIS ? …

Le livre blanc de la Défense et de la Sécurité nationale soulève une autre interrogation. Page 192, il est écrit : « *Le ministère de l'Intérieur chargé de la sécurité intérieure, ainsi que de la sécurité et de la protection civiles, dans l'acception élargie que recevront ces termes* ***dans les codes de la défense et de la sécurité intérieure*** *assurera, au niveau opérationnel, la conduite interministérielle de la crise sur le territoire* ».

Dans la nouvelle architecture de la sécurité nationale, quelle sera la place de la sécurité civile ?

ANNEXE 1 - METHODOLOGIE D'ETUDE

1. SUJET

Les systèmes d'information des SDIS et les réseaux de l'Etat

Au travers de l'infrastructure nationale partagée des transmissions (INPT) se mettent progressivement en place les « autoroutes de l'information de la sécurité intérieure ».
Au delà des infrastructures, c'est l'ensemble des systèmes d'information qui progressivement va être amené à inter-opérer.
L'étude proposée visera, à partir d'un recensement (à effectuer sous un angle prospectif) des systèmes d'information des SDIS , à projeter à l'horizon de 10 ans, les besoins d'interfaçage entre les systèmes d'information des SDIS, de l'Etat , des collectivités locales, des opérateurs ou des citoyens…
Ce travail liminaire permettra de fournir un cadre intermédiaire à la recherche menée. Un travail de recherche comparée notamment au niveau de l'UE est souhaité. Le périmètre fixé à l'issue de la phase préliminaire de l'étude, donnera ensuite lieu à un développement ciblé sur les interfaçages identifiés comme prioritaires. Ce développement à visée applicative, proposera au travers d'une proposition de plan d'action, l'ensemble des outils de conception, de pilotage et d'évaluation susceptibles d'être mis en œuvre pour satisfaire les objectifs retenus."

2. L'ANALYSE DU SUJET

Pour un néophyte, la lecture du sujet soulève de nombreuses interrogations… Beaucoup de champs sont balayés : « les systèmes d'information des SDIS », « les réseaux de l'Etat », « l'INPT », « les autoroutes de l'information », « la sécurité intérieure », « l'interopérabilité », …

Je me suis attaché dans un premier temps, à me documenter et à travailler sur ces termes et les domaines qu'ils recouvrent.

2.1 Echanges et questionnement avec le directeur de mémoire

Pour délimiter le périmètre de l'étude, j'ai procédé, dans un deuxième temps, à plusieurs échanges avec le directeur de mémoire.

Ces échanges ont porté sur :

- les termes « Systèmes d'Information (SI) », « interopérabilité », « interface (« l'arme qui unit les armes ») » ;
- le champ de l'étude ;
- le travail sur le recueil de l'existant et la prospective sur cet existant ;
- les besoins d'interfaçage (par rapport à quelles attentes ?) ;
- l'approche (prospective, globale, stratégique et non pas technologique) ;
- les « critères » d'identification des priorités d'interfaçages ;
- le « cercle » des audités ;
- les pays européens à cibler.

2.2 Reformulation du sujet

Dans un troisième temps, j'ai questionné le directeur de mémoire :

- Etant entendu que le champ de l'étude porte sur le domaine opérationnel, comment entendez-vous le terme « système d'information » ?
- Dois-je me placer dans l'optique d'un futur décret relatif à l'interopérabilité des systèmes d'information des services publics qui concourent aux missions de sécurité civile ? Y - aura-t-il une Architecture Unifié des Systèmes d' Information (AUSI) ?
- Aujourd'hui, l'Infrastructure Nationale Partagée (ou Partageable ?) des Transmissions, c'est : les relais d'ACROPOL, complétée par ceux d'ANTARES ; des Lignes Spécialisées France Telecom, des Faisceaux Hertziens THALES ; un ensemble de Commutateurs (Généraux et Secondaires) ; 2 centres de supervision. Cette description de l'INPT est-elle correcte ou bien, l'INPT, est-ce autre chose ? Un concept beaucoup plus vaste ? L'INPT représente - t'elle les futurs « réseaux de l'Etat », c'est-à-dire ceux qui répondront aux critères de l'Architecture Unifié des Transmissions (AUT) ?
- Etant entendu qu'ici, l'interopérabilité doit se comprendre comme la capacité de différents Systèmes d'Information à échanger des données, la problématique à traiter est-elle celle de la mise en réseaux des SI des services publics qui concourent aux missions de sécurité civile ?
- Considérez-vous l'INPT comme l'infrastructure destinée à être le support de l'interopérabilité des SI des services publics qui concourent aux missions de sécurité civile ?
- Le travail de recensement consiste-t-il à regarder – globalement - l'état d'avancement des SDIS dans l'organisation électronique qu'ils ont mis en place vis-à-vis de leurs informations « opérationnelles », le type d'informations qu'ils détiennent, le type d'informations dont ils ont besoin et les échanges/mises en commun à mettre en place – à l'horizon de 10 ans - avec les autres services qui concourent aux missions de sécurité civile et avec les citoyens ?
- La recherche comparée au niveau européen concerne–t-elle les déploiements d' « INPT », les SI qui y sont raccordés, les choix de gouvernance et les perspectives dans ce domaine ?
- S'agit-il de dégager les besoins (flux) d'informations qu'il faut faire remonter à l'autorité de l'Etat en situation de crise pour identifier les besoins d'interfaçages prioritaires à mettre en place ?
- J'envisage de traiter la partie « proposition de plan d'action » sous la forme « d'orientations stratégiques ». Faisant cela, est-ce que je réponds à la commande ?
- Quels sont les objectifs du plan d'actions ?
- Pour l'élaboration de ce plan d'actions, dois-je me positionner au niveau « DSC » ?
- Au-delà de « traiter un besoin national au titre de la cohérence nationale de la sécurité civile », quel est l'enjeu de l'interfaçage des SI ?
- L'objectif poursuivi est-il le pilotage des SDIS par la DSC ?
- Au nom de quoi les différents acteurs qui concourent aux missions de sécurité civile adhéreraient-ils à l'idée de mettre leurs informations en commun ? Quel serait leur intérêt ?

Ce questionnement m'a permis d'aboutir à une reformulation du sujet élaborée conjointement avec le directeur de mémoire. Cette reformulation est :

Quelles seront demain, les actions prioritaires à mettre en œuvre, visant à améliorer l'interopérabilité des Systèmes d'Information des différents acteurs concourant aux missions de sécurité civile et principalement, des SDIS ?

2.3 Intérêt du sujet

La mise en œuvre de l'interopérabilité des SI des acteurs concourant aux missions de sécurité civile présente un formidable intérêt : celui de la synergie, du « travailler ensemble » autour d'un réseau commun, pour plus d'efficacité et d'efficience au service de la sécurité de nos concitoyens.

Construire ce réseau, c'est se reconnaître autour des mêmes valeurs et partager une même mission : la protection des populations.

2.4 Champ de l'étude et limites

Le travail de recherche sur les termes du sujet et le travail d'échanges et de questionnement avec le directeur de mémoire me permettent d'établir un cadre pour l'étude.

Tout d'abord, je me situerai au niveau national, « les enjeux de sécurité civile étant une coproduction Etat/Collectivités Locales ».
Ensuite, le champ d'application sera celui de la gestion opérationnelle au sens large, c'est-à-dire tous les processus dont la finalité est la conduite d'opérations (de l'opération courante jusqu'à la conduite de crise en passant par la gestion du risque particulier).
Le travail sur l'existant (c'est-à-dire « l'état d'interopérabilité des SI ») et de prospective sur cet existant concernera les SI des « différents acteurs concourant aux missions de sécurité civile et principalement, des SDIS ».
La « pauvreté » des données disponibles, l'étendue du nombre d'acteurs concourant aux missions de sécurité civile et les contraintes de l'étude me conduiront à faire des choix que j'espère les plus pertinents possibles.
Au niveau européen, les pays ciblés seront parmi ceux ayant déployé un réseau numérique national de radiocommunications dédié aux forces de sécurité.
Les SI ne seront pas – ou peu - considérés du point de vue technologique mais plutôt en tant qu' « incarnation d'une stratégie et d'un modèle d'organisation ».
Le travail demandé n'est pas un travail sur l'INPT. L'INPT est, « *à ce jour, le premier support physique de l'interopérabilité mais l'interopérabilité des SI des services publics qui concourent aux missions de sécurité civile ne saurait se réduire à l'INPT* ». « *L'INPT est l'élément physique qui préfigure, qui supporte, la genèse de cette interopérabilité* ». « *Elle en est peut être l'alpha mais sans doute pas l'oméga* ».
« *L'INPT est un concept "hardware" qui décrit la mutualisation d'éléments physiques* ». Le travail demandé s'inscrira « *dans le concept logique plus large de l'Architecture Unifié des Transmissions (AUT)* ».
Enfin, certains aspects ne seront pas abordés ou développés tels que les problématiques juridiques liées au copyright des données, à leur élaboration/utilisation/détention vis-à-vis de la Commission Nationale Informatique et Liberté (CNIL) ainsi que les problématiques liées à la vulnérabilité (au sens « intrusif » du terme) des réseaux.

2.5 Problématiques, objectif, finalité et enjeu

Les problématiques, dégagées par l'analyse du sujet, tournent autour de la vision d'un futur réseau de sécurité civile et de sa construction :

- Comment mettre en réseau les SI des « différents acteurs concourant aux missions de sécurité civile » ?
- Quelles informations faut-il mettre en réseau ? Quels SI faut-il retenir ?
- Qui sont les différents acteurs ? Quels sont leurs intérêts ?
- Quid des modes d'organisation, notamment ceux des SDIS ? Sont-ils adaptés aux enjeux ?
- Quelle gouvernance (des SIC) ? Quel pilote ?

- Comment doit s'exprimer le rôle de l'Etat au titre de la « cohérence nationale du dispositif de sécurité civile » ?
- Par où et par quoi commencer (les interfaçages prioritaires) ?
- Quelles voies emprunter pour atteindre l'interopérabilité ?
- Quelles sont les valeurs de la sécurité civile ? Sont-elles compatibles avec les valeurs de la « société en réseaux » ?

Ce mémoire abordera ces problématiques sans pour autant répondre à toutes les interrogations qu'elles soulèvent ; certaines d'entre elles étant trop complexes voire sensibles.
Garant de la cohérence nationale, l'objectif de l'Etat est de piloter l'ensemble du dispositif de sécurité civile, autour d'un référentiel commun. Cela passe par une approche gagnant/gagnant avec tous les acteurs concernés. Gageons que c'est là que réside une grande partie de la difficulté de l'entreprise…
Au final, il s'agit d'assurer, en tout temps, aux citoyens de la Nation, une sécurité civile de qualité, experte, efficace et efficiente et ce, du niveau local au niveau national, sous l'autorité régalienne de l'Etat.
A la question « quel est l'enjeu de l'interfaçage des SI ? », le directeur de mémoire cite l'adage militaire : « *l'arme qui unit les armes* ».
Autrement dit, il s'agit bien de faire en sorte que les SI se « parlent » et par extension que les organisations travaillent ensemble. Ce faisant, au-delà du gain d'efficacité et d'efficience que l'on est en droit d'attendre de « l'unification des armes », il est un autre bénéfice qui apparaît : celui de l'augmentation du niveau de résilience pour chaque organisation, comme pour l'ensemble du dispositif « relié » de sécurité civile.
Cet enjeu – supérieur - est un enjeu de sécurité nationale. En effet, comme l'exprime le Livre Blanc de la Défense et de la Sécurité nationale, la sécurité civile – avec la sécurité intérieure - est l'une des composantes de la sécurité nationale du pays.

3. LA METHODE D'ETUDE

3.1 Recueil des données

Le recueil des données repose sur trois sources :

- Les recherches bibliographiques ;
- les auditions de personnes (entretiens) ;
- les enquêtes.

3.1.1 Les recherches bibliographiques

Elles ont consisté en la consultation et la lecture d'articles, d'ouvrages, textes et documents relatifs au sujet de l'étude. N'étant pas au départ un spécialiste des réseaux, des SI et des problématiques d'interopérabilité, un important effort d'assimilation m'a été nécessaire pour avoir une compréhension des concepts technologiques essentiels.
Complémentairement, l'audition de personnes référentes et spécialistes dans ces domaines m'a été précieuse voire indispensable.

3.1.2 Les entretiens

Compte tenu du caractère prospectif de l'étude, les données bibliographiques disponibles sur les problématiques soulevées sont faibles. J'ai donc décidé de rencontrer le plus de personnes dans la limite de mes possibilités. Le choix des personnes à auditer s'est fait avec l'accord du directeur de mémoire et bien souvent sur ses orientations. Ce guidage m'a permis de gagner un temps précieux dans la recherche du bon interlocuteur, même si, au

bout du compte, je n'aurai pas pu rencontrer toutes les personnes souhaitées. J'ai voulu privilégier le contact physique ; quand cela était impossible, j'ai procédé par rendez-vous téléphonique et, en dernier recours, par échanges de mèls.

Chronologie des entretiens et échanges (année 2009)

06 mars échange par mèl avec Monsieur Philippe DESCHAMPS, directeur de mémoire, Sous Direction des Sapeurs-pompiers et des Acteurs du Secours (SDSPAS), Direction de la Sécurité Civile (DSC) ;

09 mars échange téléphonique avec le Lieutenant-colonel Bertrand DOMENEGHETTI, chef du groupement de Libourne, SDIS 33 (Gironde) ;

09 mars échange téléphonique avec le Colonel Henri BENEDETTINI, DDSIS 11 (Aude) ;

11 mars échange par mèl avec Monsieur Philippe DESCHAMPS, directeur de mémoire, SDSPAS, DSC ;

13 mars entretien avec Monsieur Thierry COURCET, chef du Groupement des Systèmes d'Information (GSI), SDIS 64 (Pyrénées-Atlantiques) ;

31 mars entretien avec le Lieutenant-colonel Pascal DEGUDE, chef du Groupement Informatique Transmissions Téléphonie (GITT) et Monsieur Christian DUCOURNEAU, GITT, SDIS 33 ;

31 mars entretien avec le Lieutenant-colonel Dominique MATHIEU, DDA, SDIS 33 ;

31 mars entretien avec le Lieutenant-colonel Dominique BONJOUR, chef du Groupement Opérations, SDIS 33 ;

02 avril entretien avec Monsieur Philippe ARNOULD, chef du Pôle des Systèmes d'Information et de Communication, groupement Opérations, SDIS 40 (Landes) ;

03 avril entretien avec le Colonel Luc CORACK, chef de l'Etat-major de Zone (EMZ) Sud-Ouest et le Lieutenant-colonel bruno DENAVE, EMZ Sud-Ouest ;

03 avril entretien avec Monsieur Pierre MACE, directeur du Groupement d'Intérêt Public Aménagement du Territoire et Gestion des Risques (GIP ATGeRi) ;

06 avril entretien avec le Colonel Hervé DOUTEZ et Monsieur Jean-Louis LENOC, SDSPAS, DSC ;

07 avril entretien avec le Capitaine Stéphane POYAU, chef du Pôle des Méthodes Opérationnelles, groupement Opérations, SDIS 40 ;

21 avril entretien avec le Lieutenant-colonel Fabien DIDIER, EMZ Sud ;

12 mai entretien avec Monsieur Serge RAVEZ, chef du Service Zonal des Systèmes d'Information et de Communication (SZSIC) de la zone Sud-Ouest ;

18 mai entretien avec le Lieutenant-colonel Didier FORTIN, chef du groupement de gendarmerie des Landes ;

25 mai entretien avec Monsieur Alain MANDINES, société SIS (ex-EDS) ;

25 mai échange par mèl avec Monsieur Philippe DESCHAMPS, directeur de mémoire, SDSPAS, DSC ;

02 juin entretien téléphonique avec Monsieur Philippe DESCHAMPS, directeur de mémoire, SDSPAS, DSC ;

08 juin entretien avec Monsieur Robert CABE, Président du Conseil d'Administration du Service d'Incendie et de Secours des Landes, Vice-président du Conseil Général des Landes, Maire de la commune d'Aire sur Adour, et le Colonel Olivier BOURDIL, DDSIS 40 ;

09 juin entretien avec le Lieutenant-colonel Patrick HEYRAUD, DDSIS 65 (Hautes-Pyrénées), Vice-président de la Fédération Nationale des Sapeurs-pompiers de France (FNSPF), président de la commission des Systèmes d'Information et de Communication (SIC) de la FNSPF, et le Lieutenant-colonel Hervé JACQUIN, DDA 65 ;

12 juin entretien avec le Colonel Jean-Paul DESCELLIERES, DDSIS 33 et le Lieutenant-colonel Dominique MATHIEU, DDA 33 ;

16 juin entretien avec le Capitaine Gilles DUBOS, membre de la commission SIC de la FNSPF, membre du Groupe de Travail 399 (GT 399), SDIS 33 ;
16 juin entretien avec Monsieur Philippe BOUEY, SZSIC de la zone Sud-Ouest ;
17 juin entretien téléphonique avec le Commandant Eric GIROUD, animateur de la commission SIC de la FNSPF, SDIS 88 (Vosges) ;
24 juin participation à la journée de travail de la commission SIC de la FNSPF, Maison de la Fédération, Paris ;
25 juin entretien avec le Colonel Bertrand LOUARN, chef du bureau des Systèmes de Communication, Direction Générale de la Gendarmerie Nationale (DGGN) ;
25 juin entretien avec Monsieur Bertrand GOMMER, responsable Grands Comptes, société Télédiffusion De France (TDF) ;
02 juillet entretien téléphonique avec Monsieur Jean de la RICHERIE et Madame Martine COUTURIER, société EADS ;
08 juillet échange par mèl avec le Colonel François MAURER (ER), ancien président du CTIF ;
09 juillet entretien avec le Lieutenant-colonel Hervé PARIS, SDIS 01 (Ain) ;
09 juillet entretien téléphonique avec le Colonel (ER) Jean-François SCHMAUCH ;
10 juillet participation à la réunion de travail sur l'expérimentation du satellite menée par la Direction de la Sécurité Civile (DSC), l'EMZ Sud-Est, le SDIS 69 (Rhône) et le SDIS 01, préfecture, Lyon ;
10 juillet entretien avec le Colonel Serge DELAIGUE, DDSIS 69 ;
15 juillet entretien avec Monsieur Marc PELLAS, société SYSTEL ;
16 juillet entretien téléphonique avec Monsieur Bruno DOUSSINEAU, SDSPAS, DSC ;
17 juillet entretien téléphonique avec Monsieur Laurent NEISIUS, SDSPAS, DSC ;
17 juillet entretien téléphonique avec Monsieur Xavier PASCO, Fondation de la Recherche Stratégique (FRS) ;
17 juillet entretien téléphonique avec le Colonel Gilles DAUTOIS, Madame Odile FAURE-JANDET et Monsieur Philippe VIOLET, Direction des Systèmes d'Information et de Communication (DSIC) ;
20 juillet entretien avec Monsieur Pierre-Louis GAVHAM, Directeur des Systèmes d'Information (DSI) du Conseil Général des Landes ;
23 juillet entretien téléphonique avec le Colonel Claude LORON, chef du bureau des Systèmes d'Information, DGGN ;
06 août entretien avec le Docteur Eric LECARPENTIER, SAMU de France, SAMU 94 ;
07 août entretien avec le commissaire Dimitri KALININE, Service des Technologies et des Systèmes d'Information (STSI), Direction Générale de la Police Nationale (DGPN) ;
07 août entretien avec Monsieur Philippe DESCHAMPS, directeur de mémoire, SDSPAS, DSC ;
17 sept. entretien avec Monsieur Jean ROUX, Directeur territorial adjoint, ERDF-Gironde (33).

3.1.3 Enquêtes

En vue de compléter les éléments bibliographiques et les entretiens, j'ai élaboré deux enquêtes. L'une est destinée à recueillir des éléments sur l'existant au niveau du territoire national ; l'autre au niveau européen.
Pour l'enquête au niveau national, j'ai sollicité le président de la commission SIC de la FNSPF, afin de bénéficier du réseau des membres de cette commission qui sont tous des représentants régionaux.
L'enquête a été envoyée sous la forme suivante :

1. Etat descriptif sommaire des SI des SDIS de votre région ;
2. Hors du domaine technique, quelles sont, d'après vous, les conditions de l'interopérabilité ? ou pour le dire autrement, une fois les solutions techniques trouvées, quels sont les obstacles (humains, liés aux organisations, …) à la mise en œuvre de l'interopérabilité ?
3. Dans votre région, quels sont les « interfaçages » de SI existants ? Dans quel but ont-ils été réalisés ? Entre quels partenaires ? Et selon quelles règles ?
4. D'après vous, quelles sont les données détenues par les SDIS qui sont susceptibles d'intéresser un partenaire extérieur ?
   Réciproquement, quelles sont les données susceptibles d'intéresser les SDIS ? Et par qui sont-elles détenues ?
5. Dans votre région, existe–t-il un SIG régional basé sur la mutualisation et l'échange de données ?
   Si oui, sur quelle base organisationnelle fonctionne-t-il ?
   Si non, y–a-t-il un projet en ce sens ? Qui l'anime ?
6. Dans votre région, existe-t-il des projets à 10 ans, visant à améliorer l'interopérabilité des acteurs concourant aux missions de sécurité civile ?
   De votre point de vue, quels sont ceux qu'il conviendrait de lancer ?
7. L'INPT est la première « route nationale » sur laquelle des données de sécurité civile vont circuler. Demain, quels types d'échanges de données, verticaux et transversaux, voyez-vous se développer ?
8. A titre personnel, quel(s) pays européen(s) citeriez-vous comme modèle(s) en matière d'interopérabilité des SI des acteurs concourant aux missions de sécurité civile ?

Pour l'enquête au niveau européen, j'ai sollicité le Lieutenant-colonel Christophe MIGNOT en sa qualité de secrétaire général du CTIF, le Commandant Claire KOWALEWSKY de la MRI ainsi qu'un certains nombres d'officiers sapeurs-pompiers disposant de contacts européens dans leur carnet d'adresse.
J'ai contacté également tous les correspondants des pays européens apparaissant sur le site du MIC et le président du FEU (association d'officiers de sapeurs-pompiers européens).
Les pays « contactés » sont : la Suisse, l'Angleterre, l'Allemagne, la Belgique, l'Italie, l'Espagne, la Hollande, la Finlande, le Portugal, la Pologne, la Rép. Tchèque, la Grèce, ...
J'ai élaboré le mèl et le questionnaire suivants :

Mèl

Dear Sir,
My name is Jean-Marc Antonini and I am a French *fireman officer* doing a training at the ENSOSP *(National school for the officers).*
During this training I have to do a study on "The Information systems of the SDIS – French Local Fire and Rescue Departments- and the State networks."
My supervisor is Mr. Philippe DESCHAMPS from the Home Minister.
As this research includes a comparable study at the European Union level, I would be very grateful if you could help me to get in touch with people involved in the Information Systems.
Indeed I would like to know more about the infrastructures set up in your country (*radio digital* networks, exchanges between the information systems) which contribute to the interoperability of the different services.
I want to try and have a global view by dealing with the following aspects:
What strategy is adopted?
What are the objectives, the *functionalities*, the *levels of deployment,* the structures set up, their costs, the types of governance, and the evolution?
I sincerely thank you for spending time reading and answering my mail and I remain at your disposal for any further details. Yours,

Questionnaire

New-York, Madrid and London terrorist attacks have put forward the need of interoperability between the different rescue forces (fire-fighters, police, health services, army …).
The technological evolution – through the deployment of radio digital communication infrastructures and the generalisation of Information Systems within the organizations – makes this interoperability possible.

Thank you to answer to the following questions.

1) Interoperability between the Information Systems

List, for your country, the actions carried out so as to improve the interoperability between the different forces involved in civil protection. Give a global description and classify them in the following categories:

1. data acquisitions : incoming information in operational centres (emergency calls, external requests)
2. tactical : operational units with their local operational centres
3. operational : local operational centres between them
4. strategic :local operational centres with supra operational centres

2) Digital radio network for the security forces (civil protection)

a) The genesis in creating a single network dedicated to the security forces involved in civil protection (motives and adjustments to the existing situation):

b) Description of the network :
- Technology : (tetra, tetrapol, other …)
- Number of relays :
- Areas covered :
- Users (Services) :
- Population defended :
- Functionalities in operation :
- Operator (s) of the network :
-

c) Financial costs :
- Implemental costs (investment) :
- Running costs for a year :
- To be compared with the costs of former networks :
-

d) Objectives :
- Values and finalities of the project :
- Strategic Choices :
- Interoperability carried out :

e) Management :

- Financing rules :
- Types of management (governance) :
- Coordination :
- Structures set up :

f) Evolutions over the next 10 years:

3.2 Procédure d'élaboration du mémoire

Analyse du sujet

Recueil des données

Analyse par rapport au contexte (interne et externe)

Expression des valeurs/finalités

Choix du segment stratégique : « mettre en réseau les différents acteurs concourant aux missions de sécurité civile »

Analyse des forces et faiblesses (environnement interne) et des opportunités et menaces (environnement externe) en utilisant la matrice stratégique de Joseph CARLES

Plan d'action stratégique : formulation de recommandations (orientations stratégiques) avec identification des « quick wins »

3.3 Utilisation de la matrice stratégique

3.3.1 Description

La matrice « FFOM » de Joseph CARLES est une méthode d'analyse stratégique issue du milieu économique. « FFOM » est un acronyme pour « Forces, Faiblesses, Opportunités, Menaces ». L'analyse « FFOM » est une manière très efficace pour un organisme, une entreprise, … d'identifier :

- d'une part : ses **forces (F)** et **faiblesses (f)**, c'est à dire les facteurs *internes* menant à l'échec ou au succès *;*
- d'autre part : d'examiner les **opportunités (O)** qui se présentent ou les **menaces (M)** auxquels elles sont soumises, c'est à dire les facteurs *externes*.

Après un brainstorming visant à établir, pour le segment stratégique retenu, la liste des différentes « Forces, faiblesses, Opportunités, Menaces », celles-ci sont croisées afin d'établir des stratégies, de types différents, destinées à augmenter les chances futures de succès :

- stratégies de type F/O « Levier – Développement » : profiter de ses forces pour tirer profit d'une occasion externe, FAIRE SEUL ;
- stratégies de type F/M « Rempart - Défensive » : profiter de ses forces pour parer une menace, EXTERNALISER/partenariat ;
- stratégies de type f/M « Faille – Dégagement - Externalisation totale ou abandon » : palier à une faiblesse pour mieux se protéger face à une menace, NE RIEN FAIRE ;
- stratégie de type f/O « Frein - Renforcement – Organisation partenariale » : combler une faiblesse afin de ne pas rater une occasion qui va se présenter, PARTENARIAT/externalisation.

Les types de stratégie que j'identifierai à l'issue de l'analyse stratégique feront l'objet de recommandations. Celles-ci seront déclinées dans un plan d'action stratégique.

3.3.2 Tableau de synthèse des « Forces, faiblesses, Opportunités, Menaces »

	Facteurs internes	Facteurs externes
Positif	<u>Forces</u> F1 : des savoirs-faires et des compétences F2 : des dynamiques autour des NTIC (une interopérabilité en marche) F3 : une sécurité civile cohérente (autour des SDIS)	<u>Opportunités</u> O1 : l'exigence d'interopérabilité : un enjeu de l'UE O2 : l'essor des NTIC O3 : la réforme de l'AT de l'Etat O4 : des structures pour échanger
Négatif	<u>Faiblesses</u> f1 : hétérogénéité des acteurs et logique de « silos » f2 : acteurs peu ou pas sensibilisés, empêchés voire réticents/opposés (intérêts divergents) f3 : des acteurs non « reliés »qui se connaissent peu ou mal f4 : manque d' « architectes réseaux »	<u>Menaces</u> M1 : les nouveaux risques et menaces M2 : les risques des NTIC (nouvelle boîte de Pandore ?) M3 : le manque de clarification (niveau national et UE) : un frein à l'échange M4 : la puissance d'autres acteurs

ANNEXE 2 – LES THEMES DES DONNEES INSPIRE

Annexe I

1. Systèmes de référence spatiale
2. Systèmes de représentation maillée
3. Toponymes
4. Unités administratives
5. Adresses
6. Parcelles cadastrales
7. Réseaux de transports
8. Hydrographie
9. Sites protégés

Annexe II

1. Altitude
2. Occupation des terres
3. Ortho-imagerie
4. Géologie

Annexe III

1. Unités statistiques
2. Bâtiments
3. Sols
4. Usage des sols
5. Santé et sécurité des personnes
6. Services d'utilité publique et services publics
7. Installations de suivi environnemental
8. Lieux de production et sites industriels
9. Installations agricoles et aquacoles
10. Répartition de la population, démographie
11. Zones de gestion, de restriction ou de règlementation et unités de déclaration
12. Zones à risque naturel
13. Conditions atmosphériques
14. Caractéristiques géographiques météorologiques
15. Caractéristiques géographiques océanographiques
16. Régions maritimes
17. Régions biogéographiques
18. Habitats et biotopes
19. Répartition des espèces
20. Sources d'énergie
21. Ressources minérales

ANNEXE 3 – Le GIP_ATGeRI

GIP
MÉNAGEMENT DU TERRITOIRE
ET GESTION DES RISQUES

PRESENTATION DU GROUPEMENT D'INTERET PUBLIC AMENAGEMENT DU TERRITOIRE ET GESTION DES RISQUES

Constitué le 28 octobre 2005, le Groupement d'Intérêt Public Aménagement du Territoire et Gestion des Risques (GIP ATGeRi), regroupe l'Etat (Ministère de l'Ecologie, de l'Energie, du Développement durable et de l'Aménagement du territoire, Ministère de l'Agriculture et de la Pêche et Ministère de l'Intérieur, de l'Outre-Mer et des Collectivités Territoriales), les Services Départementaux d'Incendie et de Secours de la Dordogne, de la Gironde, des Landes, du Lot-et-Garonne et des Pyrénées Atlantiques, l'Association Régionale de Défense des Forêts Contre l'Incendie (ARDFCI) et les Unions des Associations Syndicales Autorisées de Défense des Forêts Contre l'Incendie ainsi que l'Office National des Forêts (arrêté du 18 novembre 2005).

Le Président est Bruno LAFON.

Le GIP ATGeRi a pour objet :

- Le développement de tous moyens propres à répondre aux missions de prévention, de prévision, de protection des milieux dans le cadre du développement durable et de la gestion des risques,
- La fourniture de données aux utilisateurs,
- La mise en place de terminaux et leur maintenance,
- La formation des personnels utilisateurs,
- L'étude et l'expérimentation de développements de produits (logiciels ou bases de données),
- Le conseil-ingénierie pour des tiers dans le domaine de la mise en place et de l'exploitation de SIG,
- La publication de rapports et études.

Les principales missions :

- Maintien et évolution du Système d'Information Géographique partagé en réseau sur 16 sites par les différents acteurs,
- Editions d'Atlas pour les différents partenaires (SDIS, ASA de DFCI, DDAF, communes…). Cette action permet aux acteurs de terrain de partager des informations identiques. Aujourd'hui plus de 100 000 cartes ont été distribuées sous forme d'atlas,
- Réalisation de cartographies, relevés de données, intégration, mise en cohérence des informations,
- Apport méthodologique pour la constitution de SIG, la collecte de données,
- Négociation avec les fournisseurs, mutualisation (logiciels, données, IGN),
- Pour mettre à jour cette cartographie et aider les services dans la collecte et l'intégration de nouvelles infrastructures, l'équipe effectue une Animation terrain et des relevés (GPS) pour la mise à jour de la cartographie DFCI,

- Administration quotidienne de la base de données SIFORA et de la base de référence GPS de Belin-Béliet pour les partenaires. Maintenance téléphonique pour l'ensemble des utilisateurs,
- Maintenance et consolidation du parc informatique du réseau SIFORA (20 postes),
- Formation des différents partenaires à l'utilisation du Système d'Information Géographique DFCI et du GPS ,
    - Formation du personnel des différents partenaires à l'utilisation des Modules métiers SIFORA : Outils Pompiers, Module Météorage, Outil gestion de chantiers…
    - Initiation et formation à la collecte de données à l'aide de matériels GPS…

L'équipe actuelle :

- Un ingénieur informaticien spécialisé réseau,
- Un ingénieur double compétence : SIG – informatique,
- Deux ingénieurs d'études,
- Un géomètre topographe spécialisé en SIG,
- Trois techniciens spécialisés en SIG topographie,
- Une secrétaire comptable.

L'ensemble est coordonné par un Directeur.

BIBLIOGRAPHIE

Les documents de travail du Sénat, série Législation Comparée 2001, *Les services d'incendie et de secours*

CHEAr 2005*, L'interopérabilité : facteur de nouvelles vulnérabilités pour les systèmes d'information de la Défense ?*

ROMAIN B. 2006, *Les SDIS : vers la technologie numérique*, Nice, Université Sophia Antipolis

2007/2/CE, *Directive Européenne INSPIRE*

CARLES J. 2007, *Gouvernance des territoires et charte managériale*, Voiron, Territorial éditions

BECHIR JL. PLATET F. D'OZOUVILLE D. 2007, *Rapport sur l'exploitation et la maintenance du système ACROPOL*

Haut Comité Français pour la Défense Civile 2008, *Constats et propositions pour une vision globale de la sécurité*, Paris, ISI Print

Direction de la Défense et de la Sécurité Civiles 2008, *Les statistiques des services d'incendie et de secours*

RIVARD F. ABOU HARB G. MERET P. 2008, *Le système d'information transverse*, Paris, Hermès Lavoisier

2008, *Défense et Sécurité nationale, le livre blanc*, Villeneuve d'Ascq, Odile Jacob

Cahier du CEREM, Hautes Etudes militaires 2008, *Repères utiles*

DESMOULINS N.2009, *Maîtriser le levier informatique*, Paris, Pearson

Délégation à la Prospective et à la Stratégie, Ministère de l'Intérieur 2009, *Prospective sur les systèmes d'information et de commandement pour la sécurité intérieure (Etude de cas des Yvelines)*

National Policing Improvement Agency 2009, *Guidance on multi-agency interoperability*

2009, *Livre blanc sur la défense et la sécurité nationale. La position de la FNSPF*