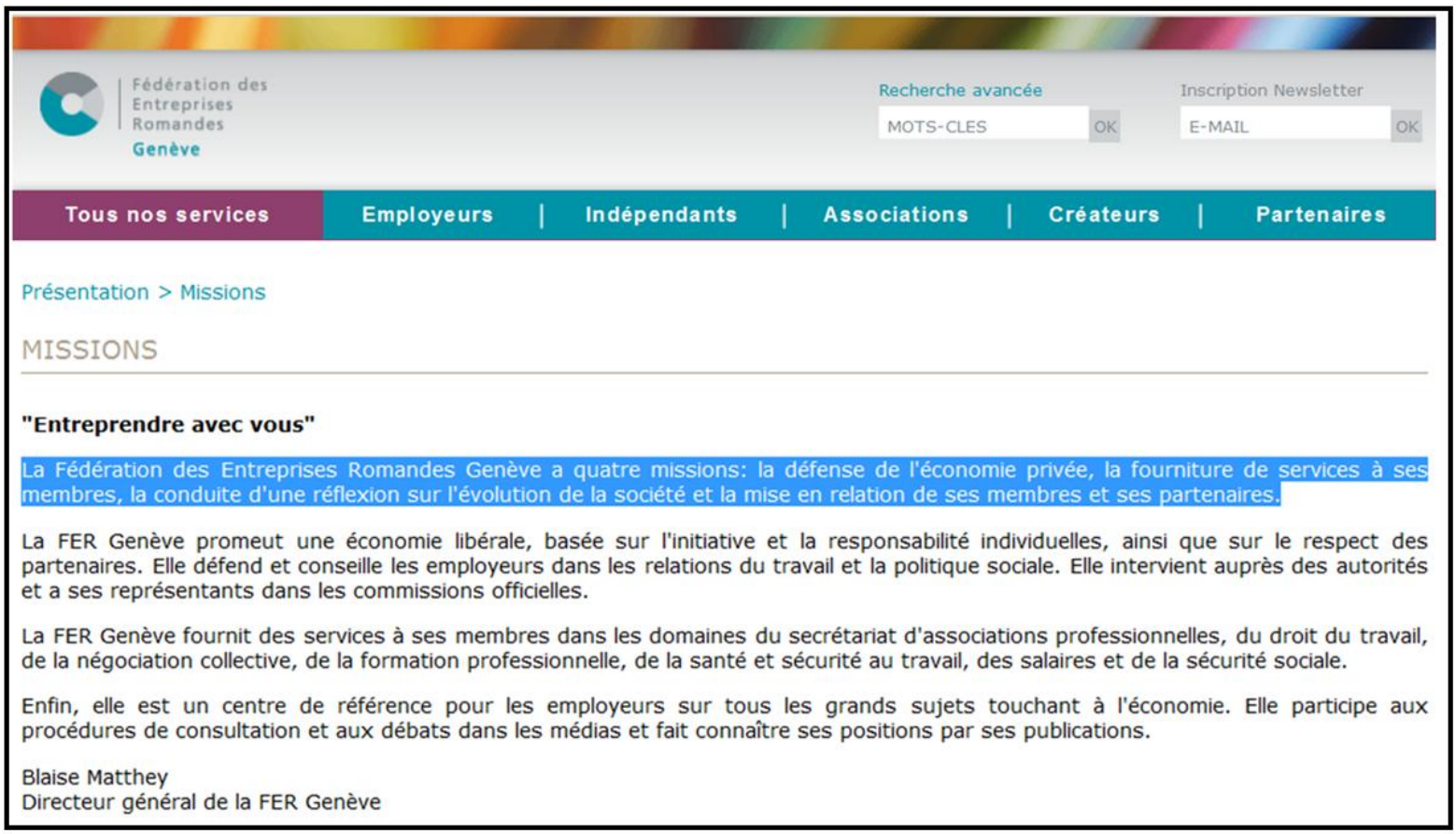
Griffes 8.5, EPFL, sécurité des données, surveillance étatique

Programme prévu du séminaire Grifes / GiTi / A3 du 8.5., EPFL.

Agenda	Thèmes	Orateurs
13h30-14h	Surveillance étatique d'Internet : Etat des lieux et comment s'en protéger ?	M. Paul Such, Ingénieur sécurité et Directeur de la société SCRT
14h-14h30	Les défis pour l'externalisation des services de sécurité	Monsieur Duilio Hochstrasser, Swisscom
14h30-15h	Cloud Computing, normes et sécurité: comment aborder les risques ?	Monsieur Antoine Coetsier, Managing Director, EXOSCALE
15h-15h15	Pause	
15h15-15h45	Attaques sur la confidentialité des données: l'expérience de MELANI.	Monsieur Mathieu Simonin, Analyste MELANI
15h45-16h15	Comment diminuer les craintes ou augmenter la confiance des clients concernant la sécurité de leurs données outsourcées ?	Monsieur Rasul Mawjee, Head of Solutions, Safe Host SA, Plan-les-Ouates
16h15-16h45	L'outsourcing et l'entreprise : Clivage et protection des données, versus garantie suffisante et économie de marché	Monsieur Raoul Diez, CSO, Fédération des Entreprises Romandes Genève
16h45-17h	Q/R	Tous
17h	Clôture	



Fédération des Entreprises Romandes Genève

Recherche avancée MOTS-CLES OK

Inscription Newsletter E-MAIL OK

Tous nos services | Employeurs | Indépendants | Associations | Créateurs | Partenaires

Présentation > Missions

MISSIONS

"Entreprendre avec vous"

La Fédération des Entreprises Romandes Genève a quatre missions: la défense de l'économie privée, la fourniture de services à ses membres, la conduite d'une réflexion sur l'évolution de la société et la mise en relation de ses membres et ses partenaires.

La FER Genève promeut une économie libérale, basée sur l'initiative et la responsabilité individuelles, ainsi que sur le respect des partenaires. Elle défend et conseille les employeurs dans les relations du travail et la politique sociale. Elle intervient auprès des autorités et a ses représentants dans les commissions officielles.

La FER Genève fournit des services à ses membres dans les domaines du secrétariat d'associations professionnelles, du droit du travail, de la négociation collective, de la formation professionnelle, de la santé et sécurité au travail, des salaires et de la sécurité sociale.

Enfin, elle est un centre de référence pour les employeurs sur tous les grands sujets touchant à l'économie. Elle participe aux procédures de consultation et aux débats dans les médias et fait connaître ses positions par ses publications.

Blaise Matthey
Directeur général de la FER Genève

1 Orateur

Fédération des Entreprises Romandes Genève

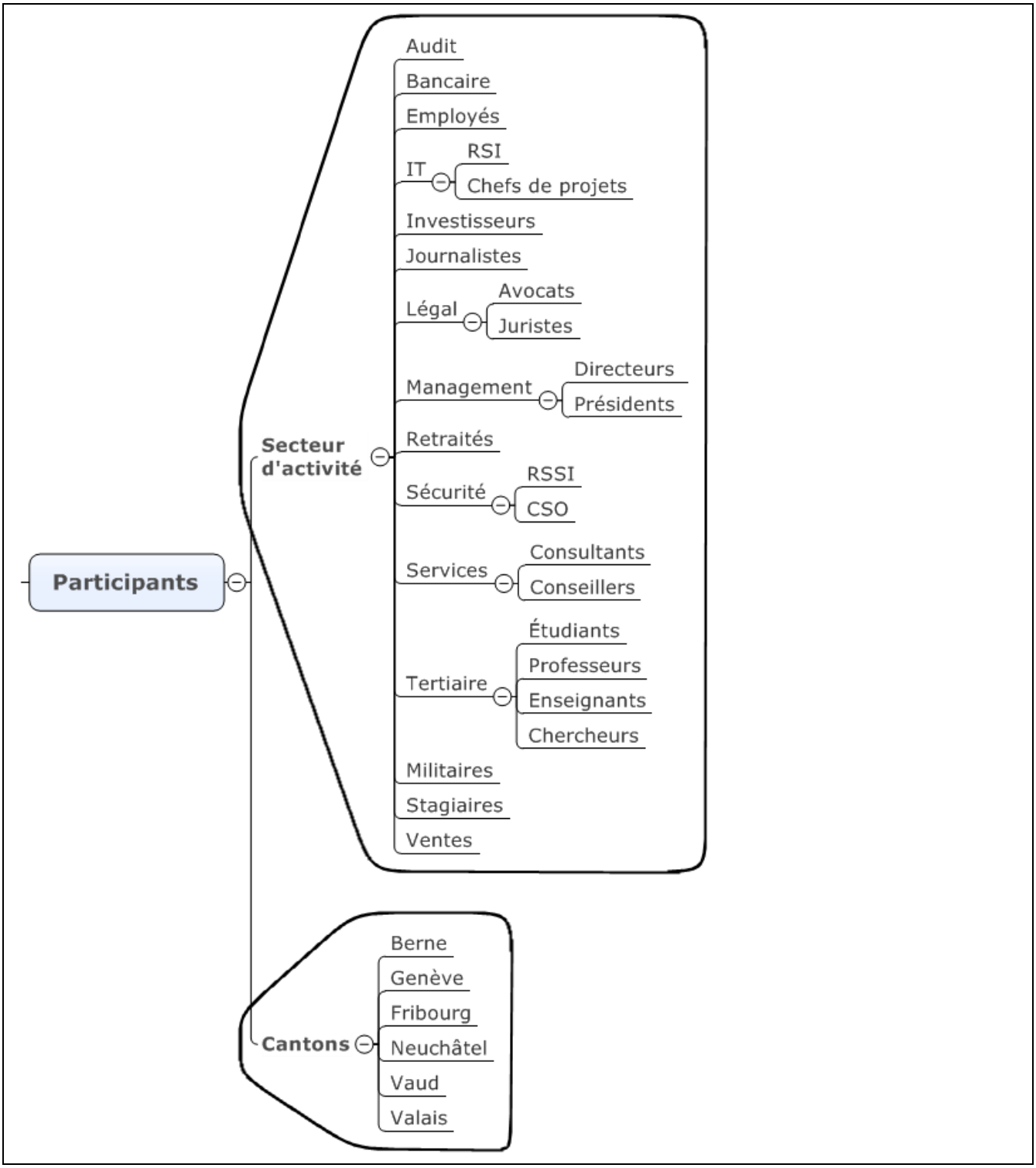
Raoul DIEZ, Directeur, Contrôle et sécurité, raoul.diez@fer-dg.ch

98, rue de Saint-Jean, Case postale 5278 - 1211 Genève 11

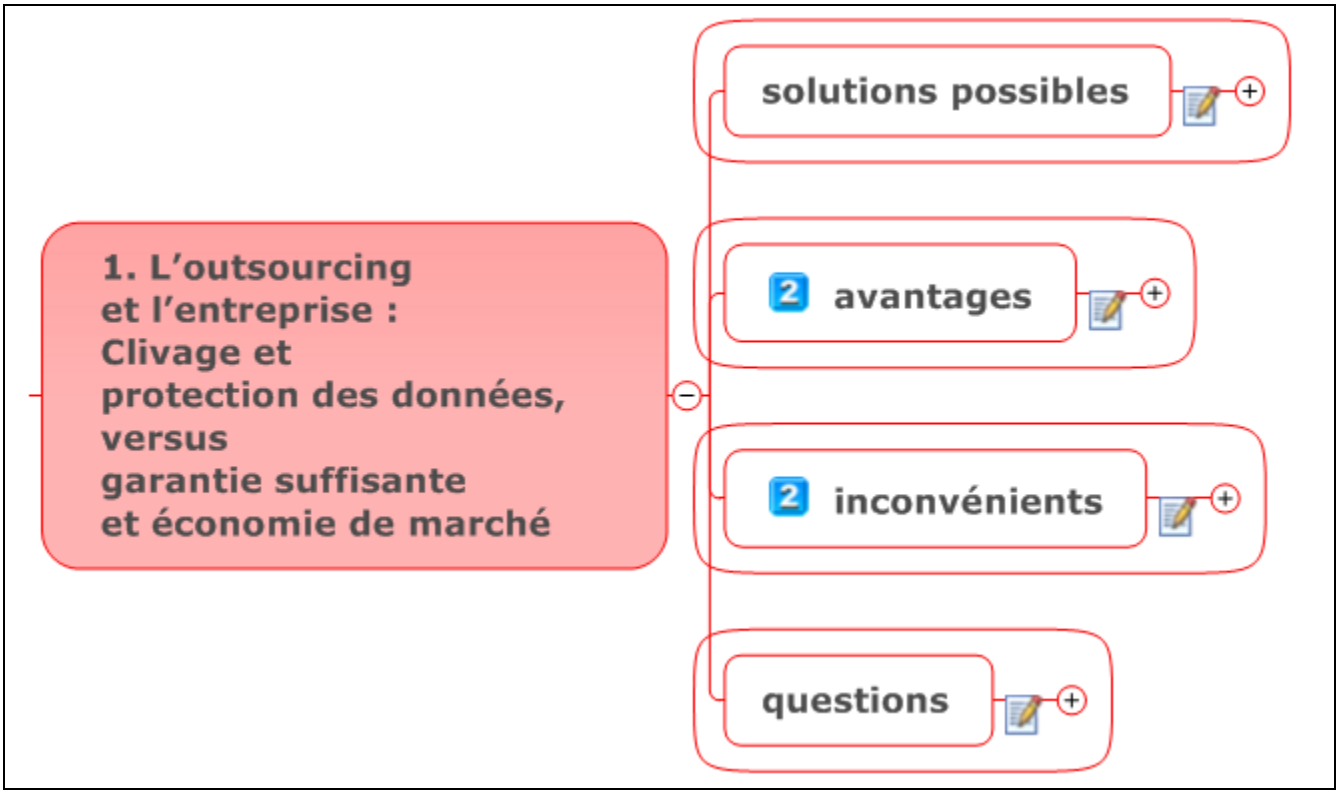
T 058 715 31 11, F 058 715 32 13

Voir le site de la FER Genève: https://www.fer-ge.ch/

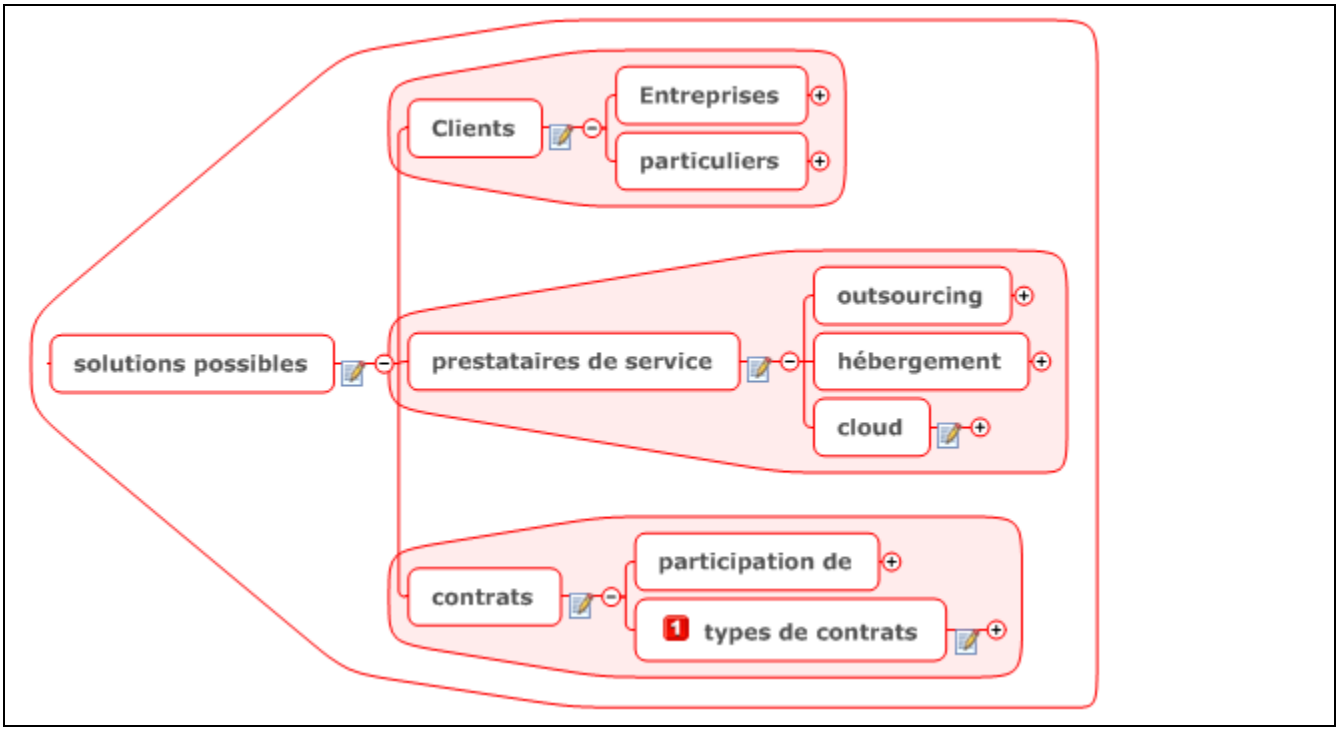
2 Participants



3 1. L'outsourcing et l'entreprise : Clivage et protection des données, versus garantie suffisante et économie de marché

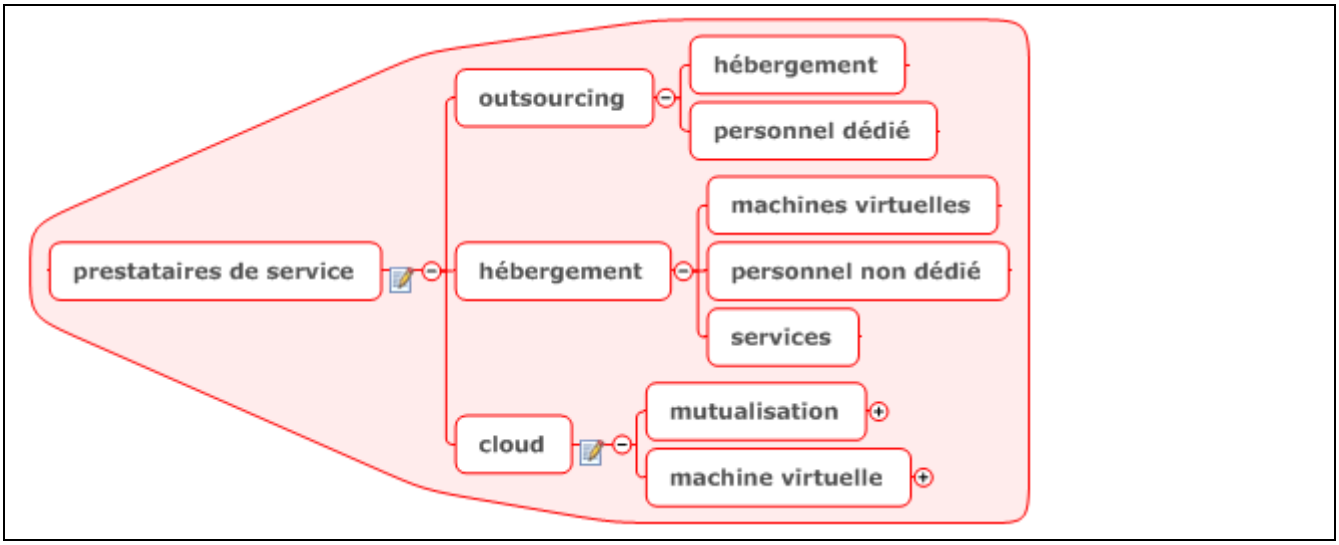


3.1 solutions possibles



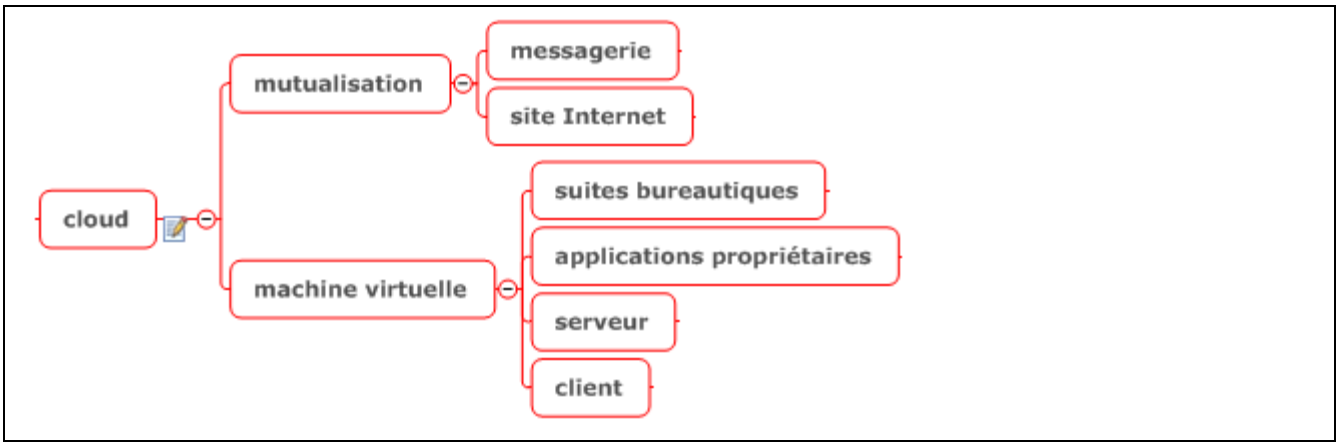
3.1.1 Clients

3.1.2 prestataires de service

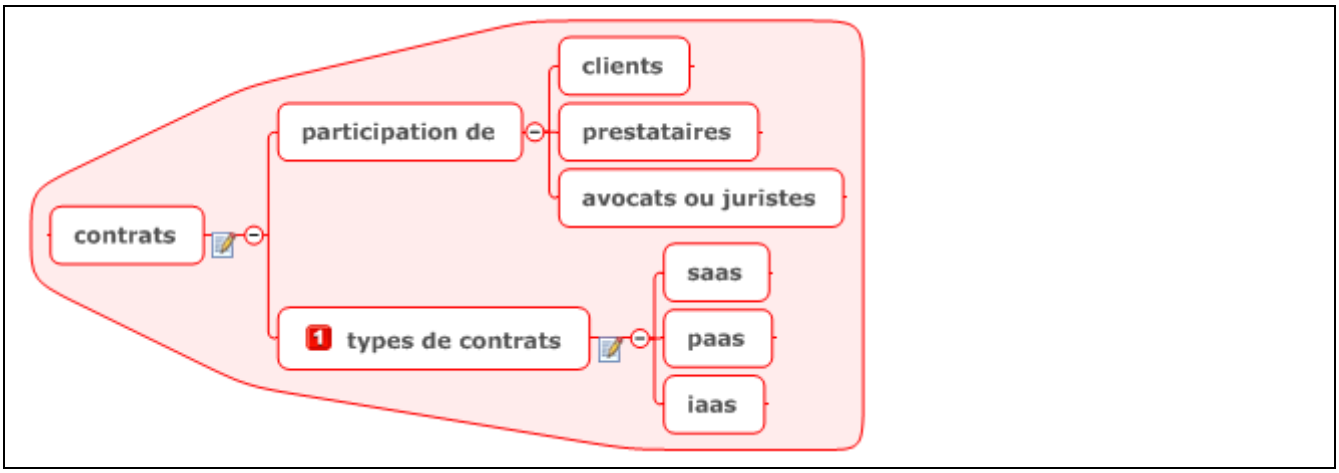


3.1.2.1 cloud

http://lentreprise.lexpress.fr/internet/le-cloud-computing-un-marche-mondial-de-29-milliards-d-euros-en-2011_30873.html

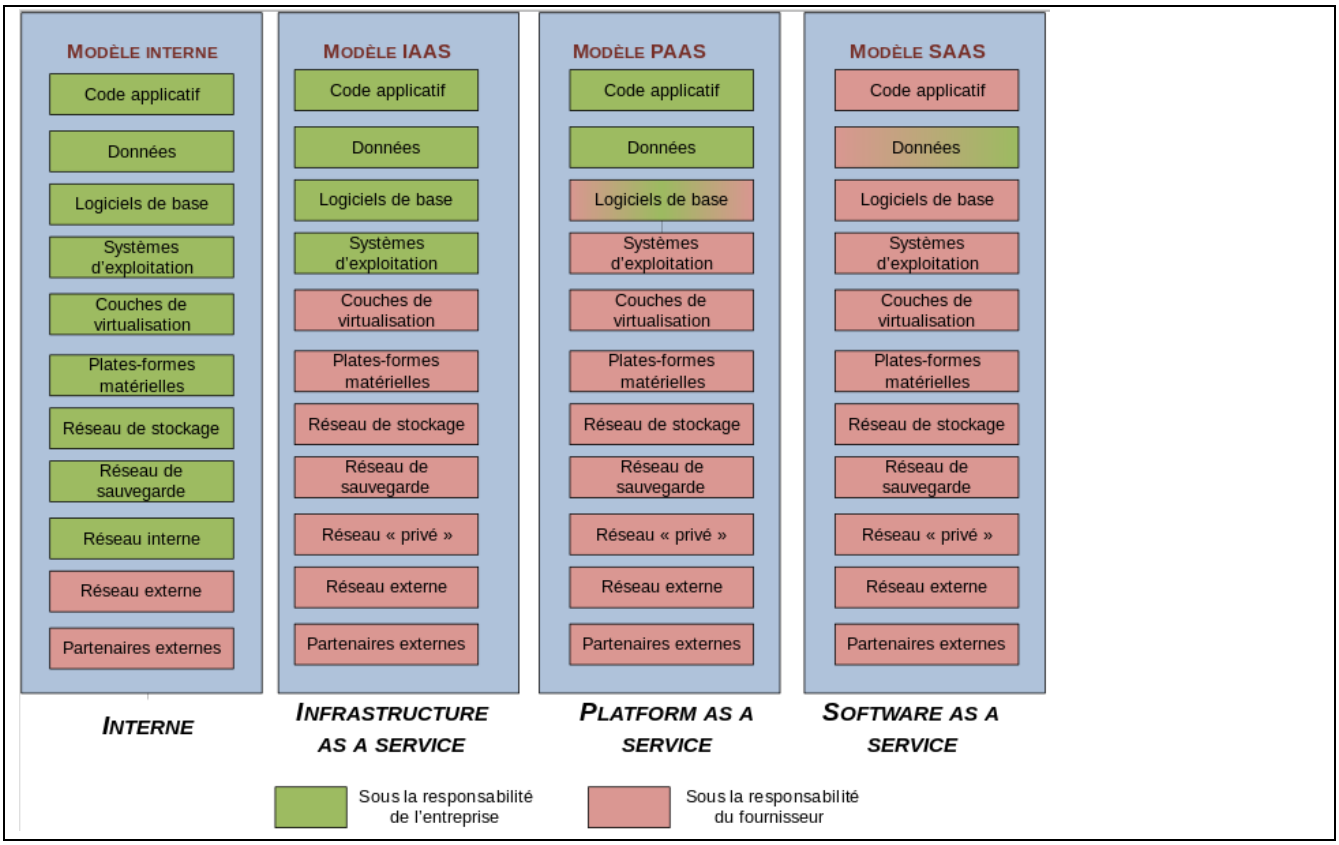


3.1.3 contrats



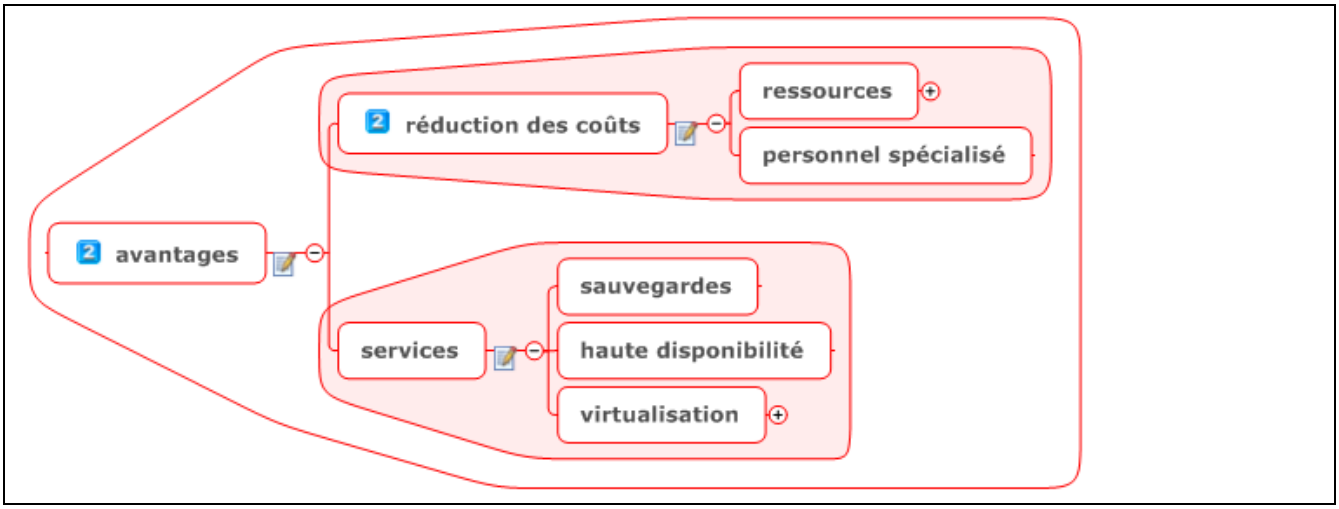
3.1.3.1 types de contrats

Voir le(s) document(s): Cloud_computing

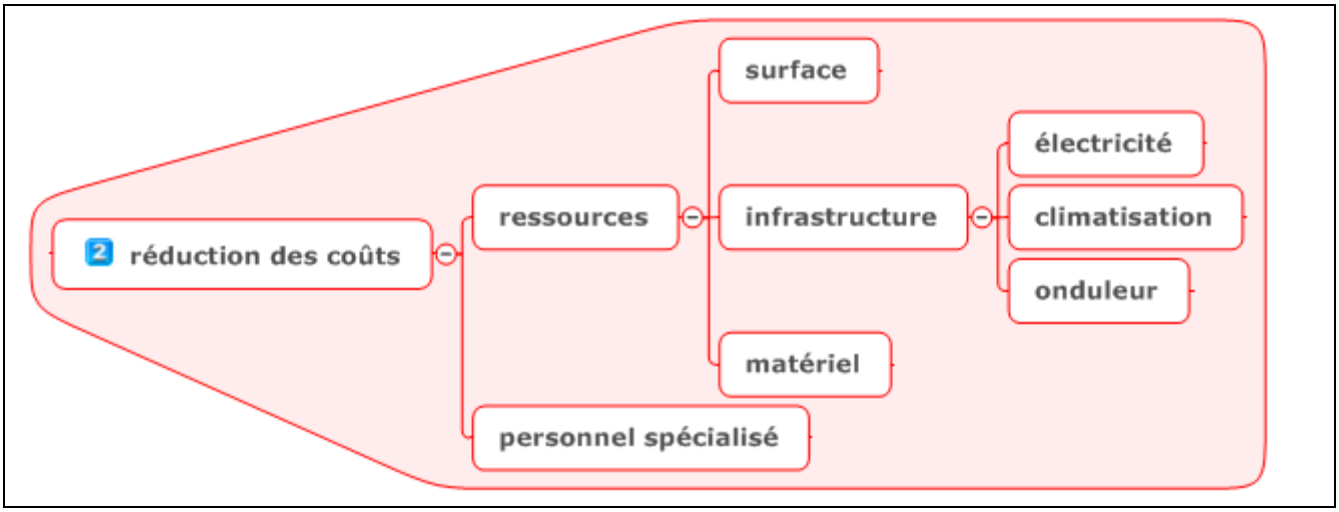


Wikipédia. Cloud Computing : http://fr.wikipedia.org/wiki/Cloud_computing

3.2 avantages

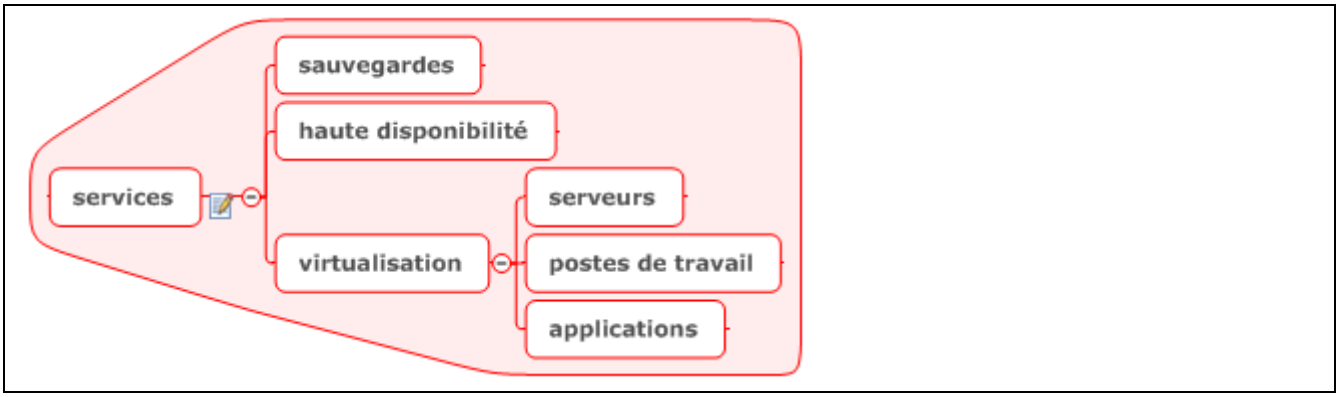


3.2.1 réduction des coûts

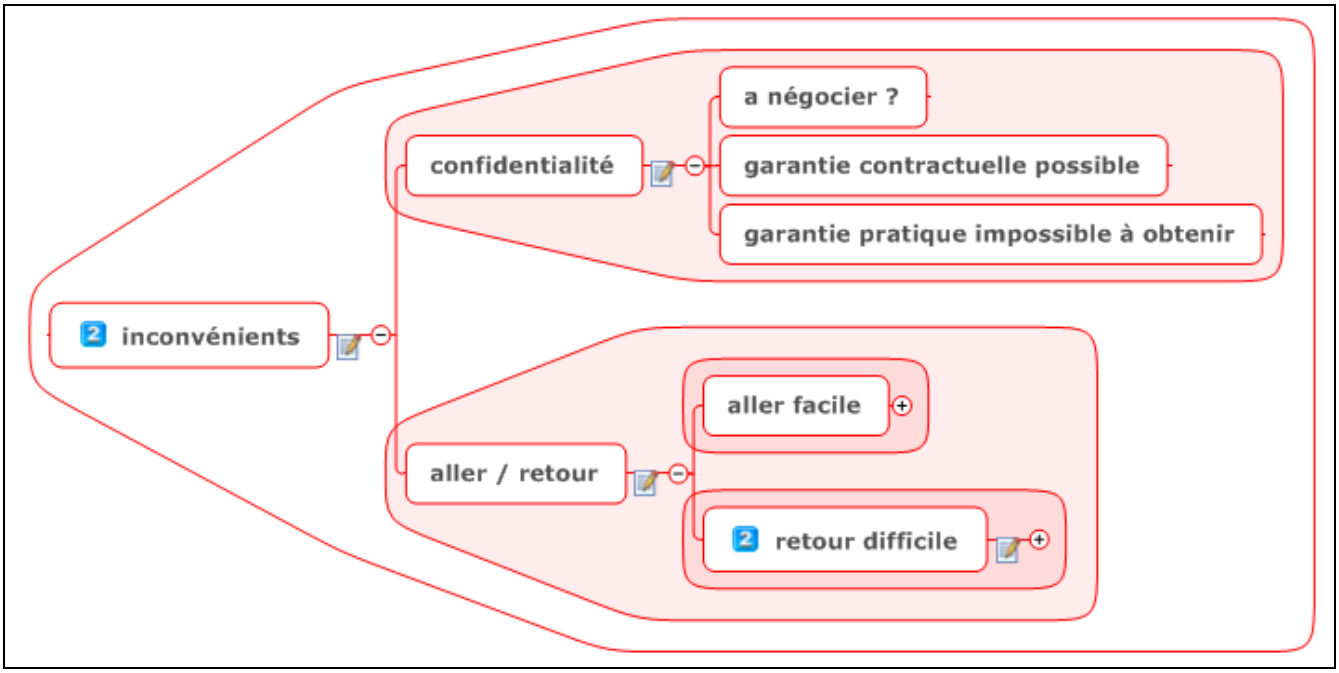


3.2.1.1 personnel spécialisé

3.2.2 services

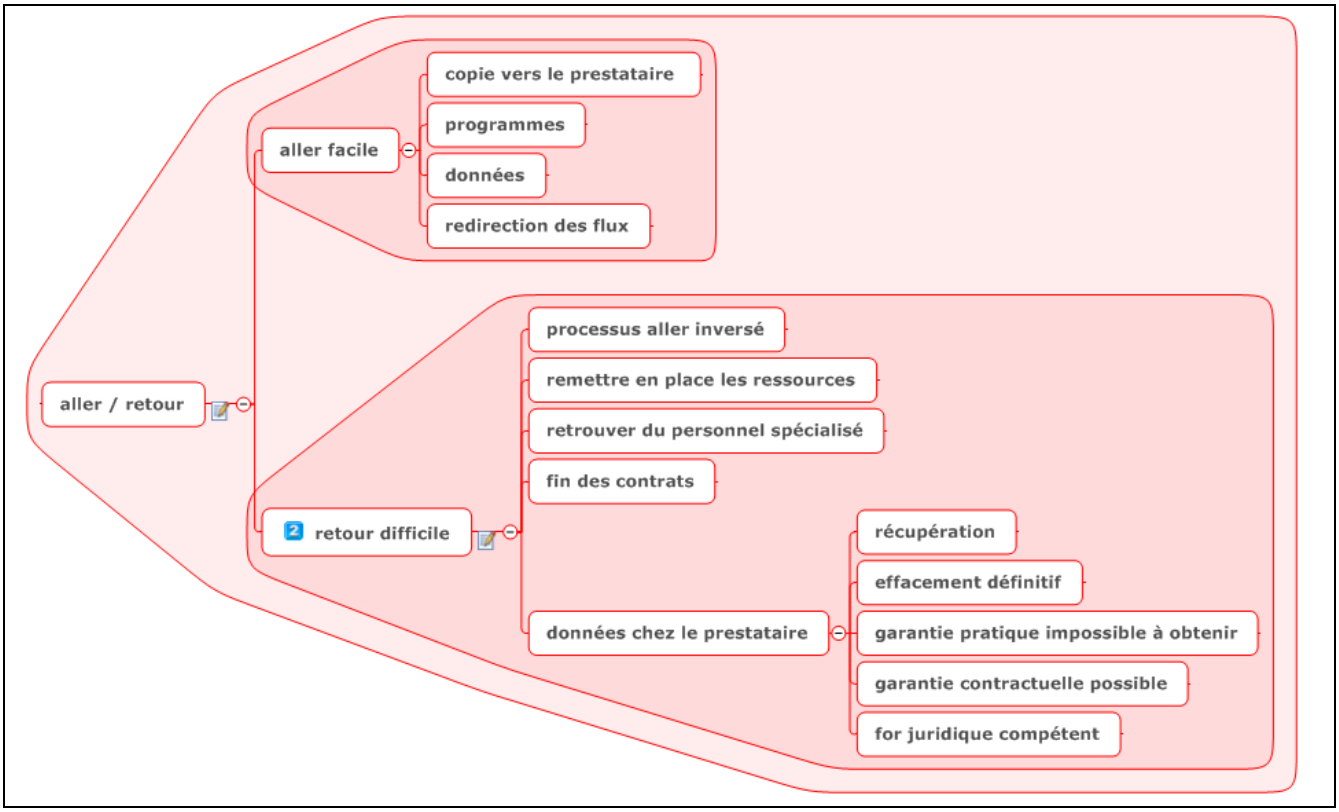


3.3 inconvénients

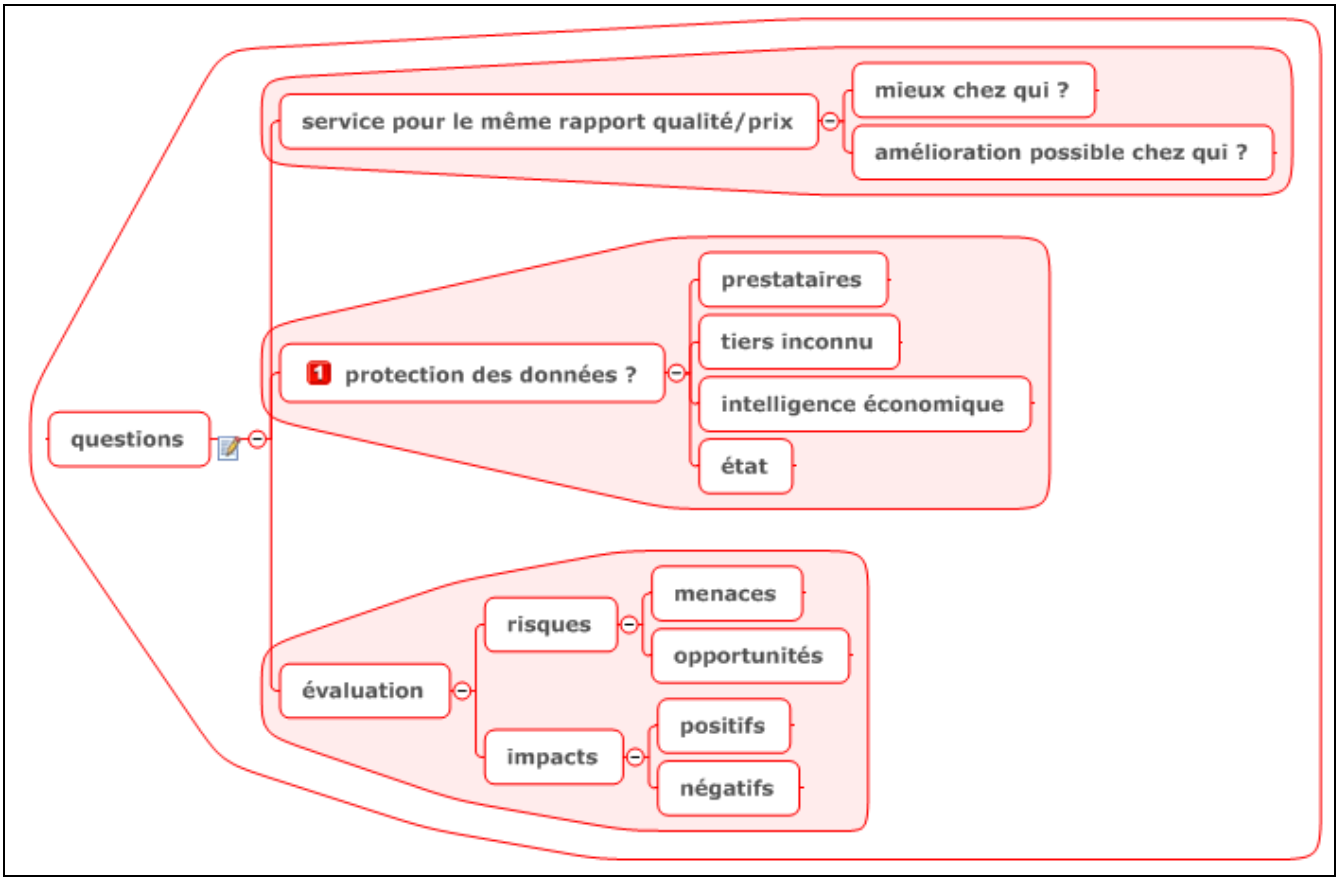


3.3.1.1

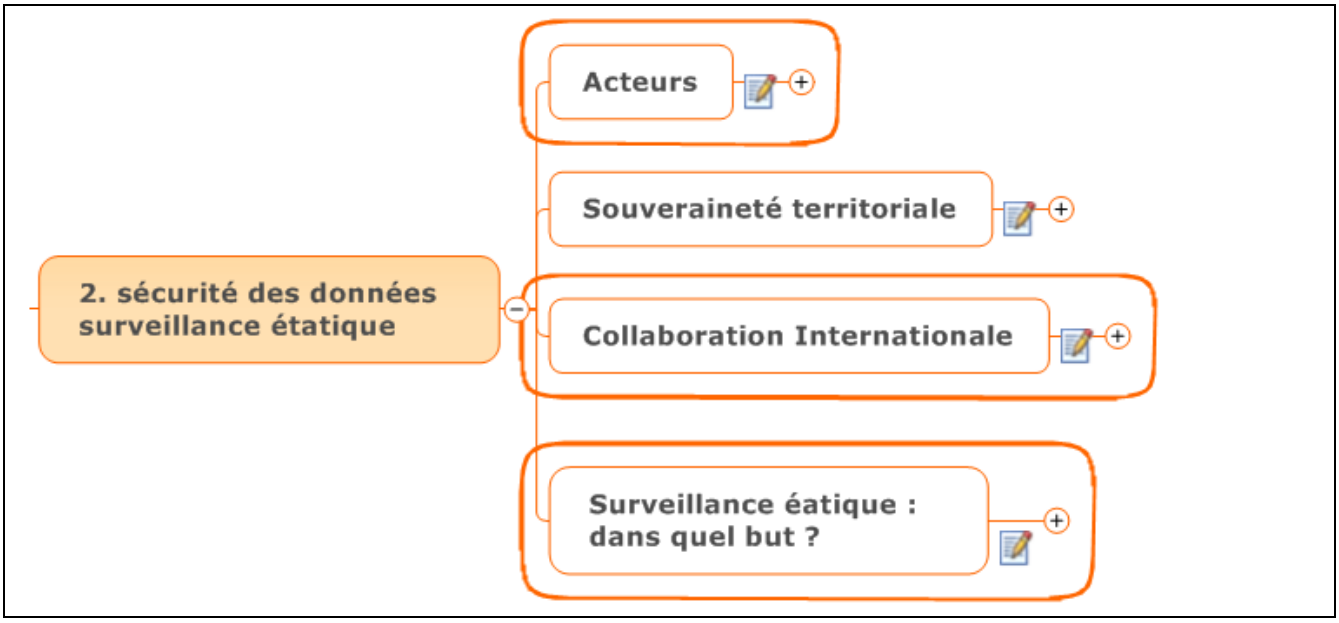
3.3.2 aller / retour



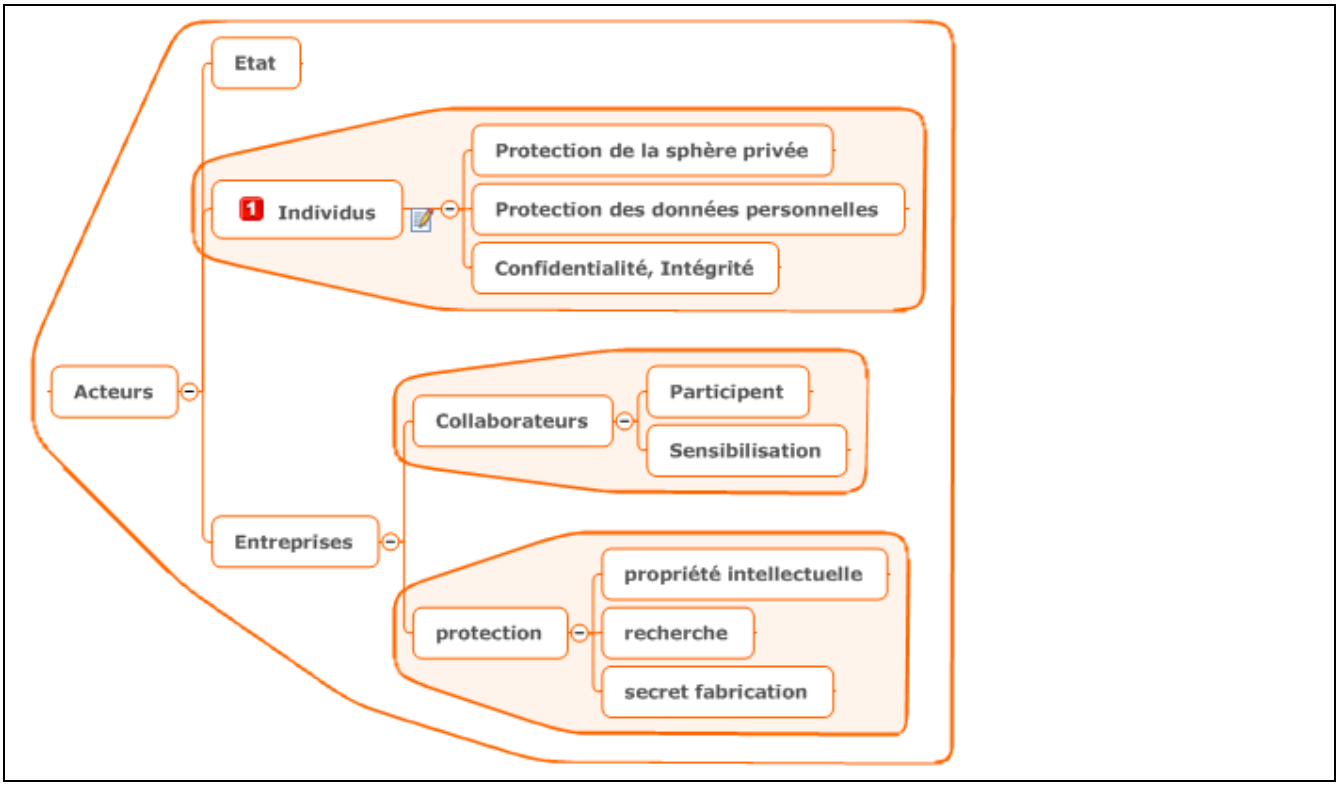
3.4 questions



4 2. sécurité des données - surveillance étatique



4.1 Acteurs



4.1.1 Etat

4.1.2 Individus

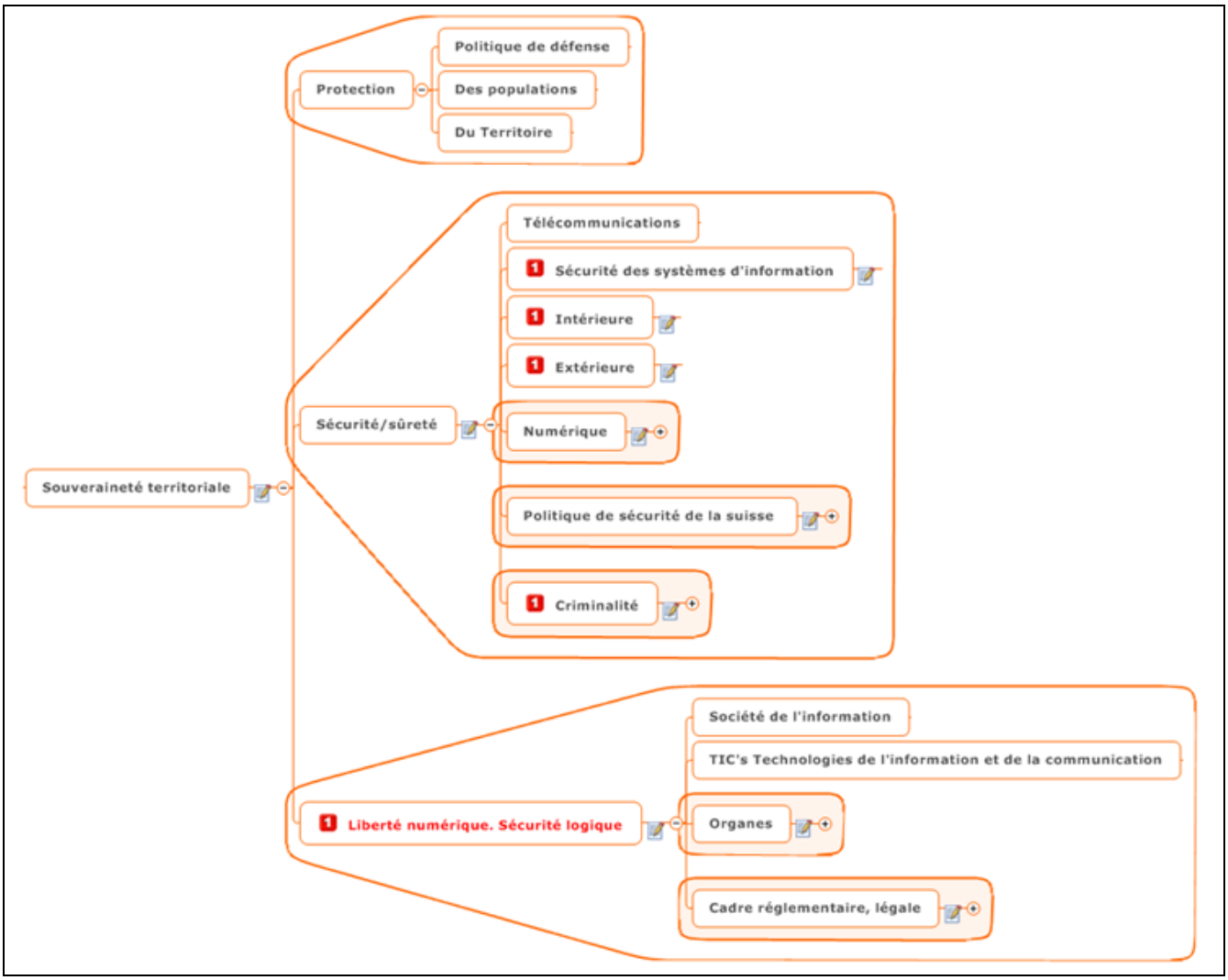
Peu importe le niveau d'abstraction, l'être humain reste au centre de la problématique. Sans rentrer dans le détail des risques directs qui l'incombent, cette approche permet de mettre en évidence certaines des règles et lois en vigueur que l'état met en place pour garantir le cadre, notamment vis-à-vis des droits du citoyen proclamés et adoptés en 1948 à travers la Déclaration universelle des droits de l'homme, adoptée par l'Assemblée générale des Nations Unies, le 10 décembre 1948, 48 états signataires : http://www.assemblee-nationale.fr/histoire/dudh/declara.asp en parlant de protection de la personne humaine (art. 3) , protection de la vie privée (12) , sécurité sociale (22), santé (25), éducation (26), droit à l'ordre social et international (28).

Et le Centre suisse de compétence pour les droits humains CSDH, qui est un acteur à signaler dans la mise en oeuvre des droits humains. Centre suisse de compétence pour les droits humains CSDH http://www.skmr.ch/frz/portrait/bref/lessentiel-en-bref.html

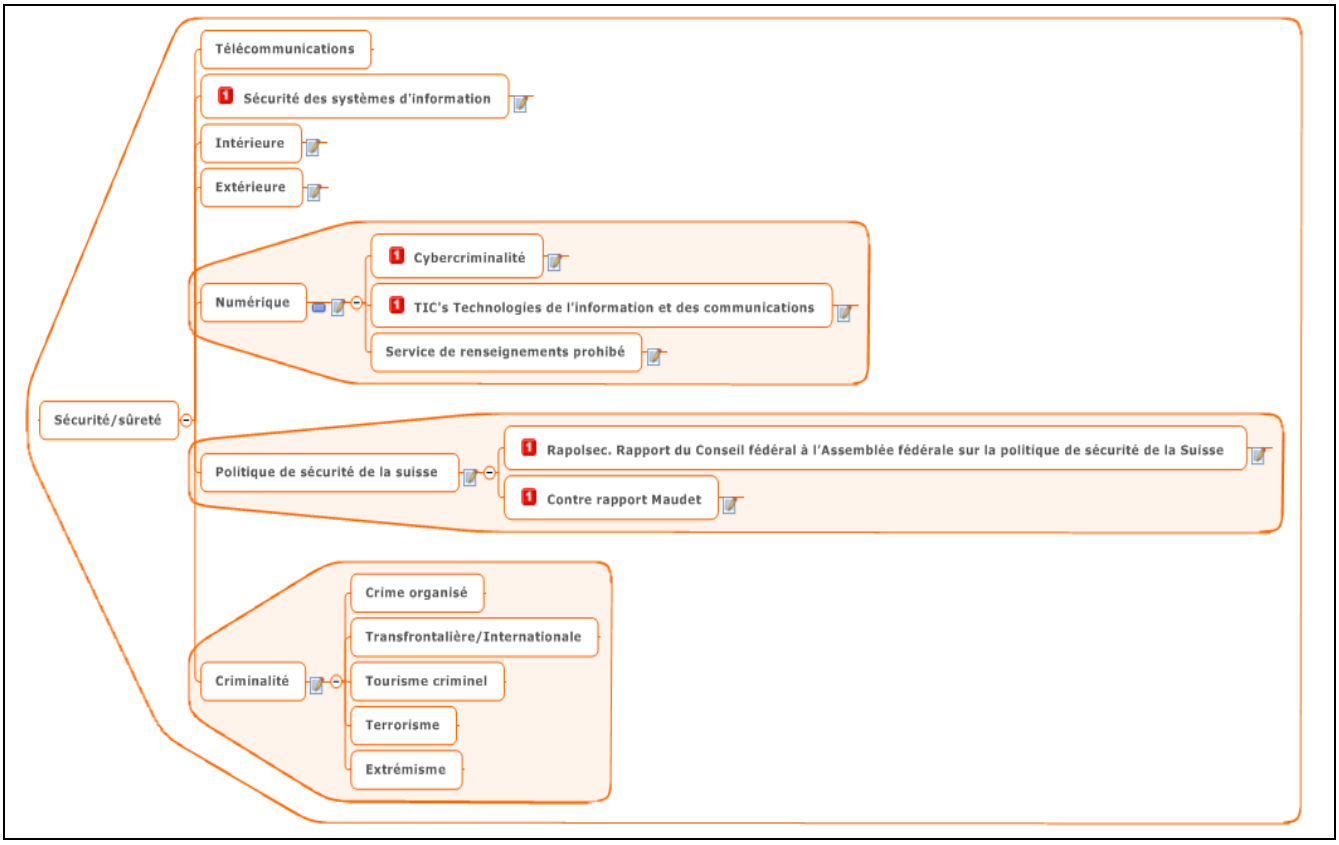
"Fait à la fois office de moteur et de facilitateur pour la mise en œuvre par la Suisse de ses obligations internationales en matière de droits humains, que ce soit au niveau communal, cantonal ou fédéral. Les compétences qu'il regroupe sont concentrées autour de six domaines thématiques : migration, police et justice, politique genre, politique de l'enfance et de la jeunesse, questions institutionnelles, ainsi que économie et droits humains"

Le cadre de **ses propres risques** est garanti donc, par l'**Etat** et aussi ses interactions avec les **Entreprises**, et ils sont représentés ici sous forme de risques **Physiques** et **Logiques.**

4.2 Souveraineté territoriale

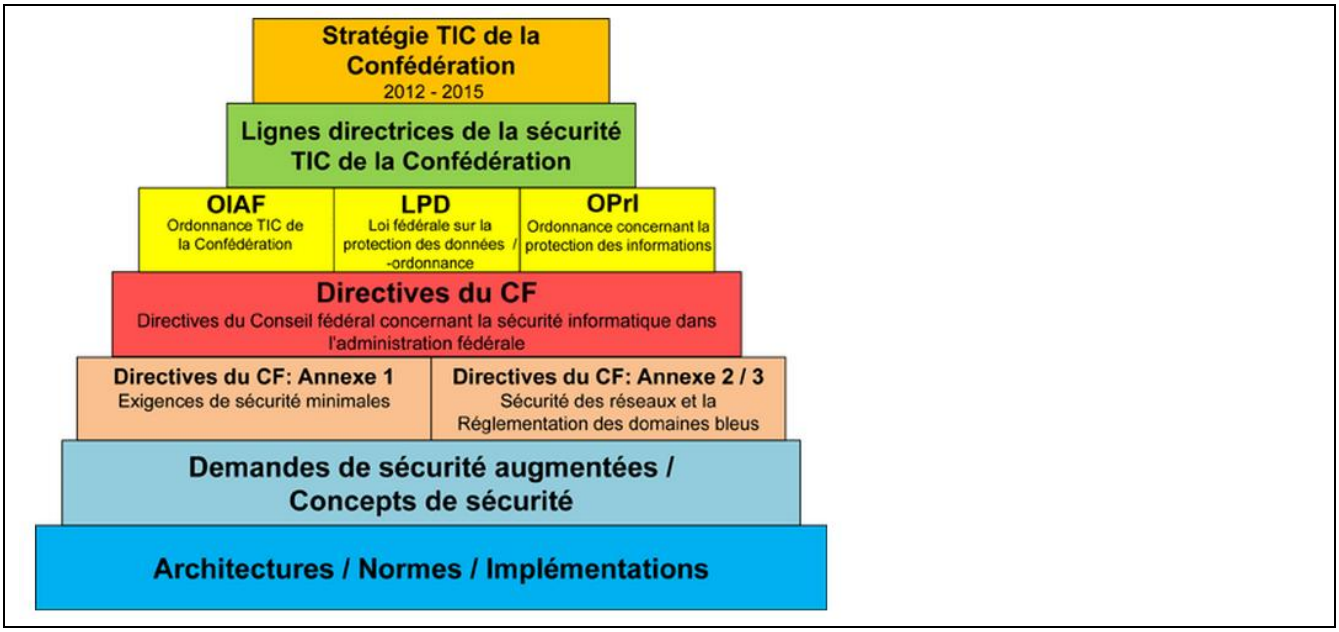


4.2.1.1 Sécurité des systèmes d'information



Voir le(s) document(s): http://www.isb.admin.ch/themen/sicherheit/00150/index.html?lang=fr

Pour gérer la sécurité des TIC's (cyberadministration), l'état, s'appui sur une structure pyramidale. A son sommet on trouve la stratégie de la confédération :



Bases de sécurité de la Confédération :
http://www.isb.admin.ch/themen/sicherheit/00150/index.html?lang=fr

Rapport du groupe de coordination Société de l'information (GCSI) au Conseil fédéral 2005 (7ème rapport)
http://www.news.admin.ch/NSBSubscriber/message/attachments/1729.pdf

4.2.1.2 Intérieure

Voir le(s) document(s): index.html, die_oe.html, innere_sicherheit.html

Intérieure

La sécurité intérieure s'appui sur l'article 185 de la constitution. "Le Conseil fédéral prend des mesures pour préserver la sécurité extérieure, l'indépendance et la neutralité de la Suisse" : Constitution fédérale de la Confédération suisse : http://www.admin.ch/opc/fr/classified-compilation/19995395/index.html#a185, via le Département fédéral de justice et police DFJP.

DFJP. Département fédéral de justice et police :
http://www.ejpd.admin.ch/content/ejpd/fr/home/die_oe.html, et concernant les principales menaces pour la Sécurité intérieure, il stipule :

"La menace envisagée sous l'angle de la sécurité extérieure ou intérieure s'est totalement modifiée. Le caractère transfrontalier des risques et dangers s'est accentué. On trouve, au cœur du phénomène, le développement de la criminalité organisée et du tourisme criminel transnational. L'imbrication matérielle et géographique accrue des domaines de menace requiert la mise en œuvre de nouvelles parades. Ce n'est qu'au prix d'une coopération internationale soutenue qu'il sera possible de lutter avec effet contre les menaces émanant du terrorisme, de l'extrémisme violent, du service de renseignements prohibé, de la prolifération et de la criminalité dans le domaine du nucléaire, de la criminalité organisée, ainsi que de l'abus des technologies modernes de l'information"

DFJP. Département fédéral de justice et police. Sécurité interieure : http://www.ejpd.admin.ch/ejpd/fr/home/themen/sicherheit/innere_sicherheit.html

4.2.1.3 Extérieure

Voir le(s) document(s): home.html, 19995987

Le DFJP travaille en étroite collaboration avec le Département fédéral des affaires étrangères DFAE. Département fédéral des affaires étrangères : http://www.dfae.admin.ch/eda/fr/home.html, notamment pour ce qui est des dispositions communes.

DFJP. Ordonnance sur l'organisation du Département fédéral de justice et police (art 5) : http://www.admin.ch/opc/fr/classified-compilation/19995987/. A noter que la Suisse préside l'Organisation pour la sécurité et la coopération en Europe OSCE à partir de 2014. OSCE. Organisation pour la sécurité et la coopération en Europe : http://www.osce.org/. La Suisse répond ainsi à une des priorités de sa politique étrangère, à savoir l'engagement en faveur de la stabilité en Europe et dans les régions limitrophes.

4.2.1.4 Numérique

4.2.1.4.1 Cybercriminalité

Voir le(s) document(s): cybercriminalite-la-suisse-engage-28-specialistes-dans-la-lutte-contre-les-cyberrisques-566-1185868

http://www.arcinfo.ch/fr/suisse/cybercriminalite-la-suisse-engage-28-specialistes-dans-la-lutte-contre-les-cyberrisques-566-1185868

15.05.2013, 12:02 - Suisse
Actualisé le 15.05.13, 12:11

Cybercriminalité: la Suisse engage 28 spécialistes dans la lutte contre les cyberrisques

INFORMATIQUE

La Confédération va créer 28 postes supplémentaires de spécialistes dans la lutte contre les cyberrisques. Crédit: KEYSTONE

Ajouter un commentaire
Tous les commentaires (0)

La Suisse va lutter plus activement contre les cyberrisques. La Confédération va ainsi créer 28 nouveaux postes de personnes spécialisées dans le domaine.

La Confédération va créer 28 postes supplémentaires de spécialistes dans la lutte contre les cyberrisques. L'armée sera également appelée en renfort. Ce renforcement découle du plan de mise en oeuvre de la stratégie nationale adopté mercredi par le Conseil fédéral.

Le plan, qui comprend seize mesures devant être mise en oeuvre d'ici fin 2017, souligne la nécessité de renforcer les effectifs. Bien que la stratégie exclue les cas de guerre ou de conflit, le gouvernement a décidé d'appeler les militaires en renfort. Les capacités existantes de l'armée lui permettent à titre subsidiaire de participer à la réduction des cyberrisques.

Coordination fédérale

Vu qu'un grand nombre de tâches de la Confédération sont concernées et que la stratégie sera mise en œuvre de manière décentralisée, le Conseil fédéral a en outre mis sur pied un comité interdépartemental de pilotage.

Celui-ci sera chargé de coordonner les activités requises au niveau de l'administration fédérale, des cantons et du secteur privé. Il observera l'évolution des cyberrisques et soumettra des recommandations au gouvernement.A terme, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) assumera une fonction de coordination et de direction au niveau opérationnel. D'ici 2017, elle sera la plaque tournante de l'information sur les cyberrisques.

Surveillance constante

Les mesures décidées ont pour but de renforcer la prévention ainsi que la gestion de la continuité et des crises. Les conditions de base essentielles restent la responsabilité individuelle, la collaboration au niveau national entre les milieux économiques et les autorités ainsi que la coopération avec l'étranger.

Le plan définit des calendriers pour les mesures à prendre et précise quels sont les organes compétents. Les capacités techniques permettant de surveiller constamment les réseaux de la Confédération devront ainsi être créées avant la fin de 2015.

L'organe de coordination devra par ailleurs présenter d'ici fin 2013 un premier aperçu de la nécessité urgente de légiférer. Un concept destiné à combler les lacunes jugées prioritaires sera soumis au Conseil fédéral au plus tard à fin 2014.

L'office fédéral de la police élaborera de son côté, et en collaboration avec les cantons, un concept de gestion avec vue d'ensemble globale des infractions. But affiché : les cantons se prononceront au troisième trimestre 2015.

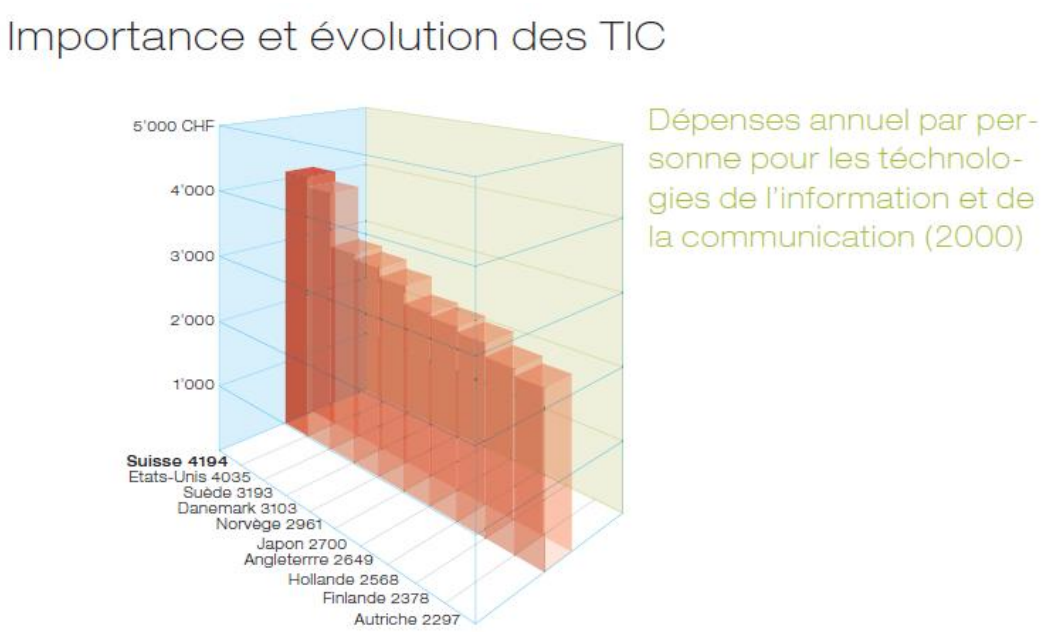
Source: ATS

4.2.1.4.2 TIC's Technologies de l'information et des communications

Voir le(s) document(s): ind16.indicator.30104.160301.html, ind16.Document.25563.xls, index.html, index.html

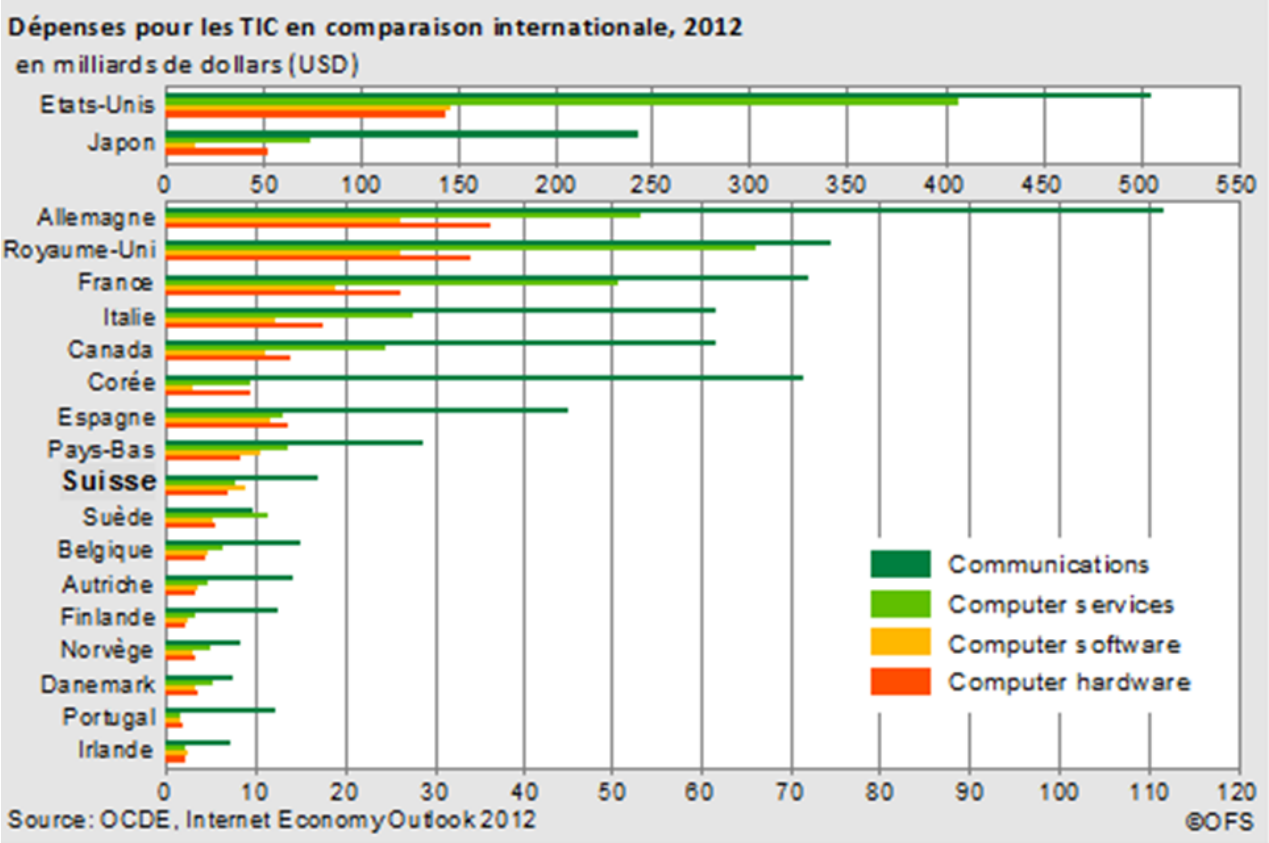
TIC's Technologies de l'information et des communications

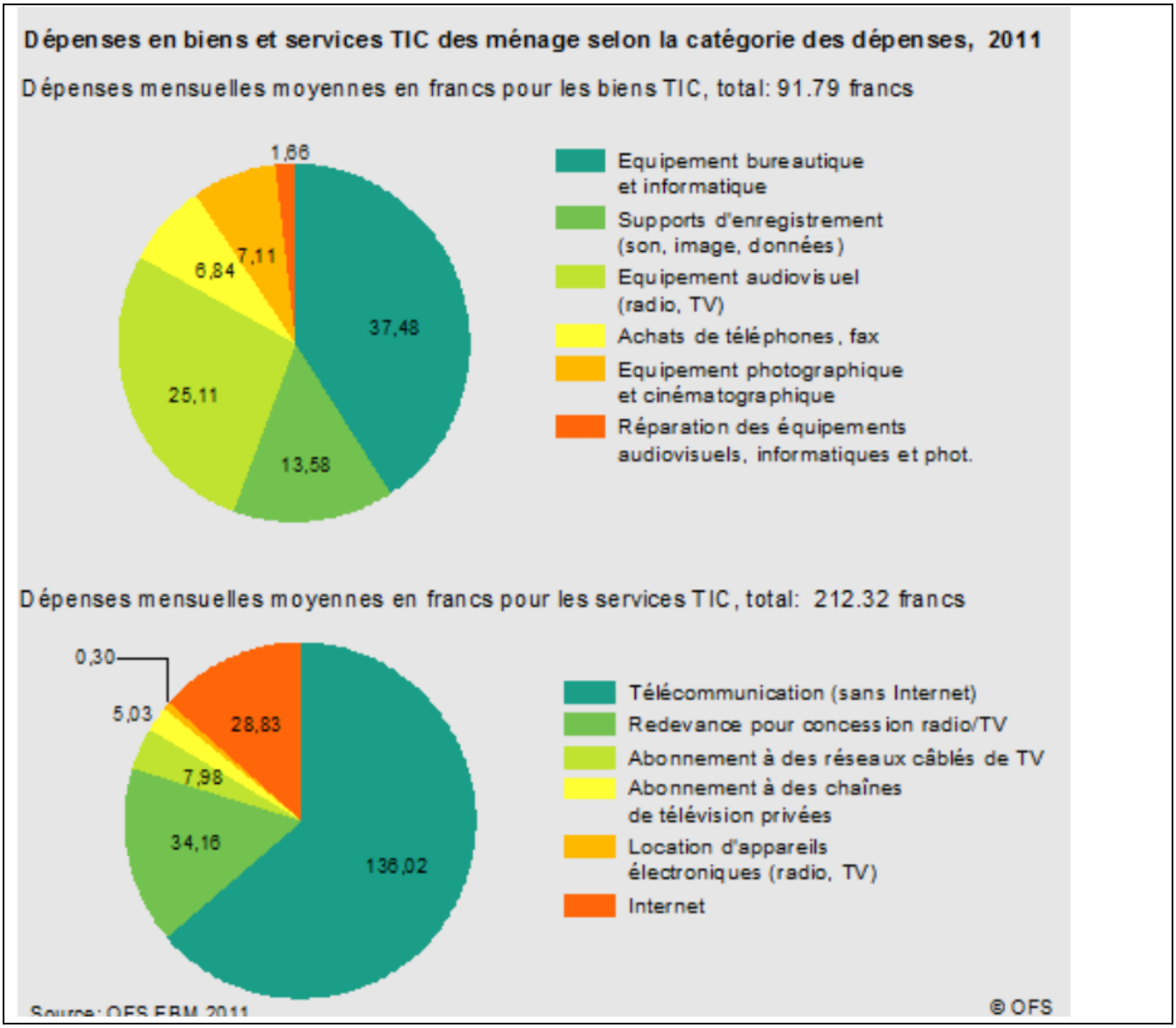
Touchant la sûreté des TIC's, il existe en suisse un cadre organisationnel et opérationnel qui fait référence dans le monde. En l'an 2000 déjà, les statistiques prouvaient que les dépenses annuelles par personne en suisse, dépassaient même les investissements effectués aux USA.



http://www.bfs.admin.ch/bfs/portal/fr/index/themen/16/03/key/ind16.indicator.30104.160301.html

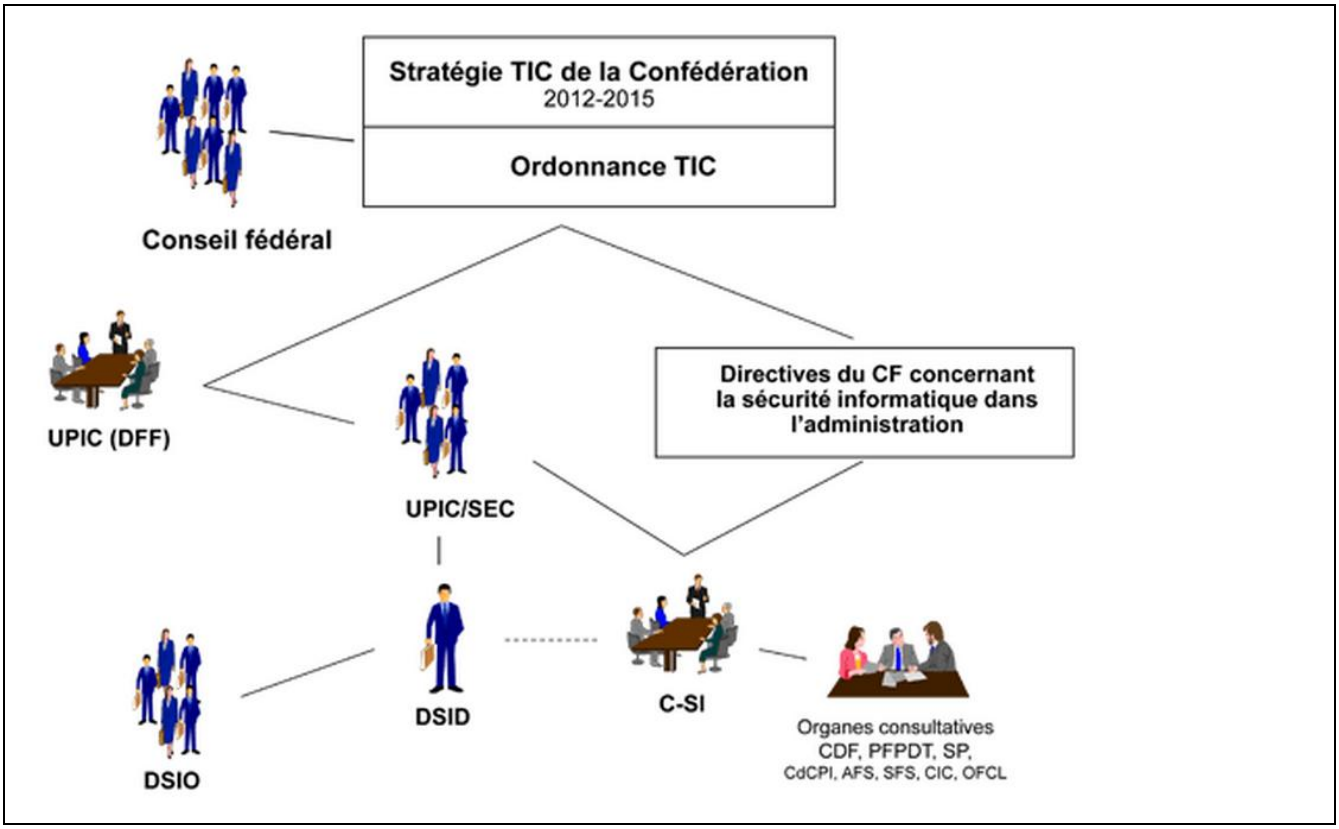
Selon les calculs repris par l'OCDE, en 2012, les dépenses annuelles totales dans les technologies de l'information et de la communication s'élèvent en Suisse à 41 milliards de dollars. La Suisse se caractérise par un très haut niveau de dépenses TIC, puisqu'elle devance les pays de taille comparable tels l'Autriche et la Suède par exemple.
Les Etats-Unis, avec 1'201 milliards de dollars de dépenses TIC, sont de très loin le premier pays de l'OCDE en termes de dépenses TIC, suivis du Japon (385 milliards) et de l'Allemagne (227 milliards).
En proportion du PIB cependant, la Suisse se place au 1èr rang des pays de l'OCDE avec 10% du PIB, devant le Japon (9%) et les Etats-Unis (8%).





http://www.bfs.admin.ch/bfs/portal/fr/index/themen/16/03/key/ind16.Document.25563.xls

Société de l'information vulnérable. Le défi de la sûreté de l'information, Page 15 *:*
http://www.isb.admin.ch/dokumentation/publikationen/00162/index.html?lang=fr



Organisation de la stratégie TIC de la Confédération

Société de l'information vulnérable - Le défi de la sûreté de l'information, Ruedi Rytz, octobre 2002 :
http://www.isb.admin.ch/dienstleistungen/publikationen/index.html?lang=fr

4.2.1.4.3 Service de renseignements prohibé

Service de renseignements prohibé

La Division Enquêtes Protection de l'Etat de la Division principale Police judiciaire fédérale (PJF) est chargée des infractions contre l'Etat :
http://www.fedpol.admin.ch/fedpol/fr/home/fedpol/organisation/bundeskriminalpolizei.html

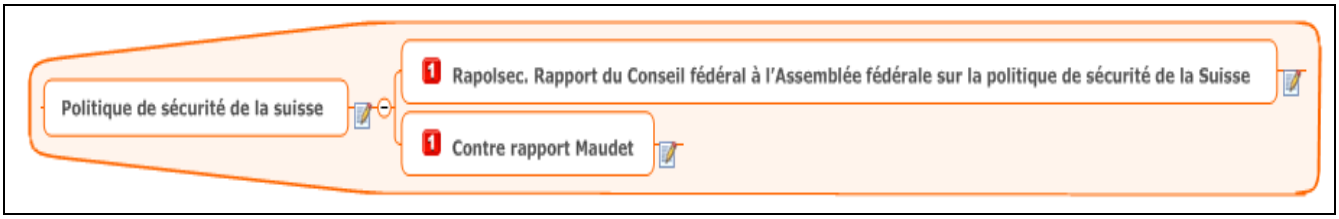
"La Division Enquêtes intervient en cas de soupçons d'activités d'espionnage politique ou économique, de prolifération de moyens de destruction massive et d'infractions relevant du droit pénal international (crimes de guerre, génocide et crimes contre l'humanité). Elle enquête également dans les cas suivants: délits liés aux explosifs, infractions contre les devoirs de fonction, faux monnayage et cyberattaques contre les infrastructures de la Confédération"

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

Mesures concrètes réparties en sept champs d'action

DDPS. Stratégie nationale de protection de la Suisse contre les cyberrisques. Page 4: http://www.news.admin.ch/NSBSubscriber/message/attachments/27334.pdf

Politique de sécurité de la Suisse :



4.2.1.4.4 Rapolsec. Rapport du Conseil fédéral à l'Assemblée fédérale sur la politique de sécurité de la Suisse

Voir le(s) document(s): sipolbf.pdf

Rapolsec. Rapport du Conseil fédéral à l'Assemblée fédérale sur la politique de sécurité de la Suisse

http://www.vbs.admin.ch/internet/vbs/fr/home/documentation/bases/sicherheit.parsys.5013.downloadList.36678.DownloadFile.tmp/sipolbf.pdf

10.000

Rapport
du Conseil fédéral à l'Assemblée fédérale sur la politique de sécurité de la Suisse

du 23 juin 2010

Il établit que les engagements de surveillance, de protection et de sûreté effectués en Suisse

4.2.1.4.5 Contre rapport Maudet

Voir le(s) document(s): Politique-de-s%C3%A9curit%C3%A9-Le-vrai-rapport1.pdf

Contre rapport Maudet

http://www.pierremaudet.ch/site/wp-content/uploads/2013/03/Politique-de-s%C3%A9curit%C3%A9-Le-vrai-rapport1.pdf

POLITIQUE DE SECURITE SUISSE

> LE VRAI RAPPORT

Pierre Maudet
Conseiller administratif de la Ville de Genève
en charge du Département de l'environnement urbain et de la sécurité

4.2.1.5 Criminalité

Voir le(s) document(s): jabe-2012-f.pdf

La lutte contre le risque lié à la criminalité n'est plus uniquement une affaire interne. La mondialisation touche aussi la criminalité, qui s'étend, traverse les frontières, devient pluraliste et touche tous les aspects de l'économie physique et numérique.

C'est le département fédéral de justice et police DFJP qui gère les risques liés à la criminalité, via son office fédéral de la police Fedpol.

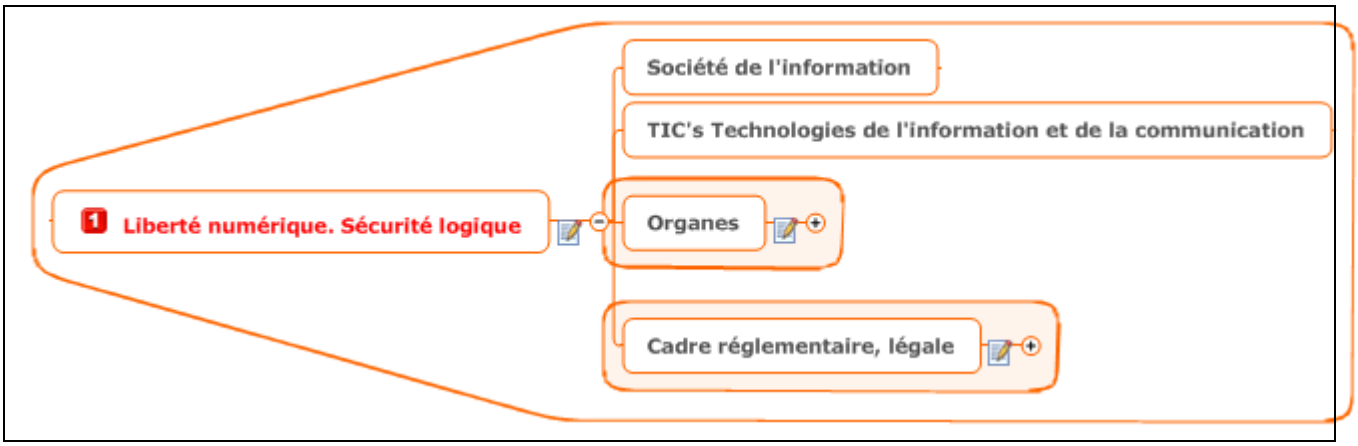
La classification des risques criminels physiques amène le Fedpol à publier de rapports annuels d'appréciation et d'évaluation de la situation.

Fedpol. Lutte de la confédération contre la criminalité :
http://www.fedpol.admin.ch/content/dam/data/sicherheit/jahresberichte/jabe-2012-f.pdf

Le dernier rapport dresse un bilan de la situation sur les différentes manifestations du crime :

- Crime organisé
- Criminalité économique et blanchiment d'argent
- Stupéfiants
- Traite d'êtres humains
- Trafic de migrants
- Fausse monnaie
- Trafic illicite de biens culturels
- Cybercriminalité
- Violence lors de manifestations sportives
- Sécurité des personnes et des bâtiments
- Terrorisme et extrémisme violent

4.2.2 Liberté numérique. Sécurité logique



Sommes-nous au bon niveau d'abstraction pour parler des risques numériques? En d'autres termes, la sécurité logique pourrait devenir une affaire d'état ?

L'informaticien Snowden, à travers ses révélations sur l'existence d'une surveillance massive des réseaux numériques à l'échelle planétaire, qui devait à l'origine permettre la protection du territoire (TIC's et territoire étroitement liées) crée l'environnement propice aux interrogations suivantes :

- Est-il possible de parler de protection des technologies de l'information comme faisant partie de la souveraineté de l'état?
- Devons-nous considérer les TIC comme une richesse essentielle devant être placée par l'état à la croisée de la population et du territoire?
- Est-il suffisant de parer aux risques "*d'une manière adéquate*" ?
- Devons-nous classifier les TIC comme une menace, un risque potentiel, un risque avéré, ou une opportunité? ou bien les quatre à la fois?
- Si c'est une opportunité -comme on aurait tendance à le comprendre- quel est le prix que la société est prête à accepter de payer?

L'état tente de répondre à la problématique à travers la Société de l'information : "Le Conseil fédéral encourage la société de l'information en Suisse. Le Conseil fédéral est conscient de l'importance fondamentale que revêtent les technologies de l'information et de la communication (TIC) pour les citoyens et l'économie suisses. En 1998 déjà, il a adopté une stratégie pour la société de l'information en Suisse. Celle-ci a été actualisée en 2006 et en 2012.

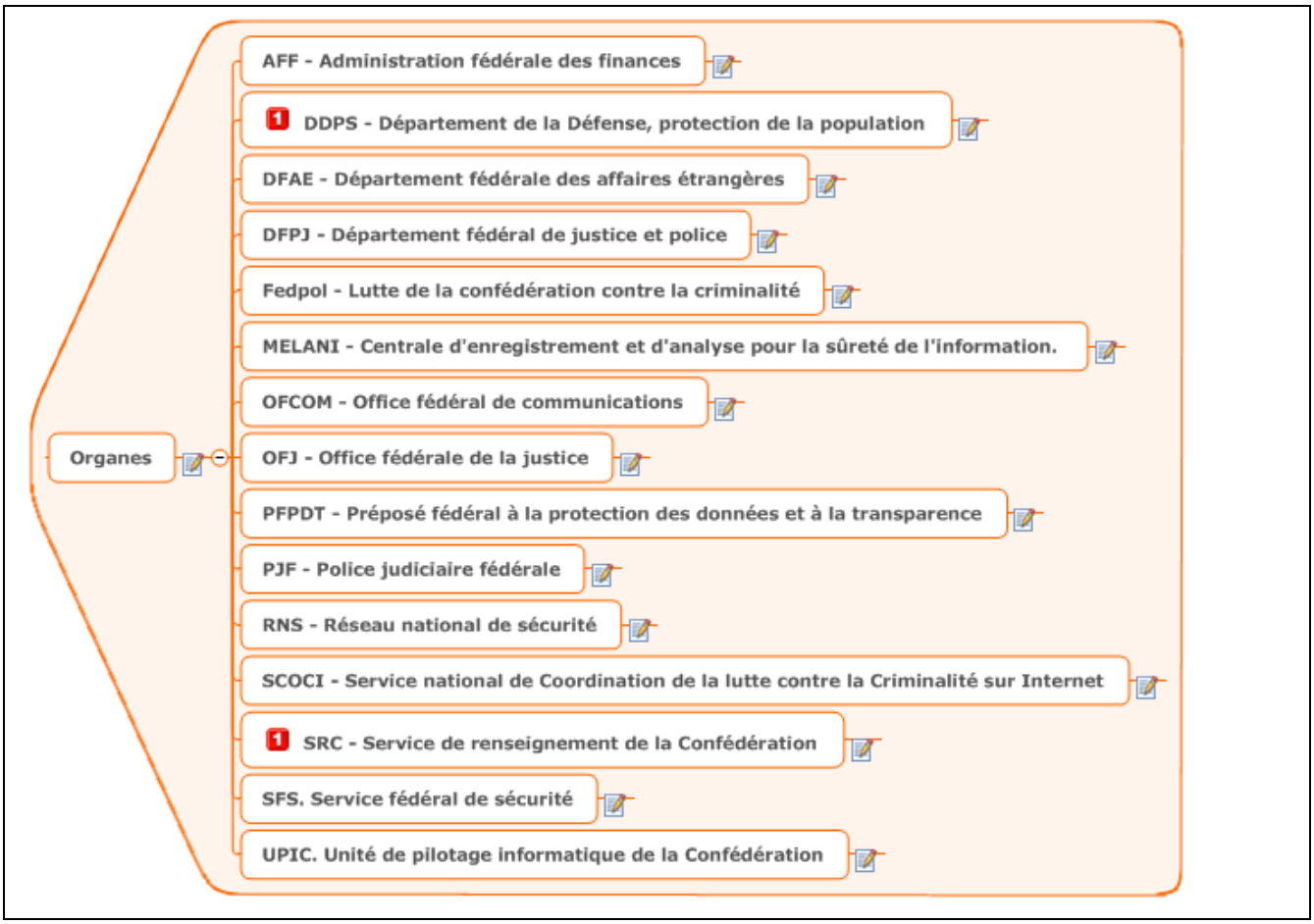
Dans sa nouvelle stratégie, le Conseil fédéral définit les champs d'action où le potentiel novateur des TIC peut particulièrement déployer ses effets. La stratégie est déterminante pour l'activité de l'administration fédérale. Les axes prioritaires de la Confédération y sont fixés.

La stratégie pour une société de l'information est appliquée de manière décentralisée dans les départements fédéraux. Le Conseil fédéral a chargé un "Comité de pilotage Société de l'information" d'assurer la mise en oeuvre coordonnée et ciblée ainsi que le développement de la stratégie. Une "Direction opérationnelle" implantée à l'Office fédéral de la communication (OFCOM) soutient les travaux du comité" (OFCOM. Office fédéral de la communication : http://www.bakom.admin.ch/themen/infosociety/index.html?lang=fr)

"Le Conseil fédéral veut exploiter les avantages qu'offre l'utilisation des TIC pour la Suisse, tout en parant aux risques de manière adéquate. Par la présente stratégie, il tient compte de l'évolution des TIC et des nouveaux défis à relever, et s'engage activement pour façonner la société de l'information." (Stratégie du Conseil fédéral pour une société de l'information en Suisse.
http://www.bakom.admin.ch/themen/infosociety/00695/index.html?lang=fr)

L'état met à disposition des statistiques sur la société de l'information :
http://www.bfs.admin.ch/bfs/portal/fr/index/themen/16/04.html

4.2.2.1 Etat. Organes



4.2.2.1.1 AFF - Administration fédérale des finances

AFF. Administration fédérale des finances : http://www.efv.admin.ch/f/index.php

L'outil de recherche mis à disposition par l'AFF, donne 400 résultats sur le mot risques. Droit, législation, politique, documentation, questions, mandats, etc., tous les thèmes sont abordés.

AFF. Recherche avancée :
http://www.efv.admin.ch/f/suche/index.php?queryString=risques&urlOption=0&queryLanguage=fr&displayLang=fr&Button+Suche=Recherche

4.2.2.1.2 DDPS - Département de la Défense, protection de la population

Voir le(s) document(s): departement.html

DDPS. Département de la Défense, protection de la population et sports : http://www.vbs.admin.ch/internet/vbs/fr/home/departement.html

4.2.2.1.3 DFAE - Département fédérale des affaires étrangères

DFAE. Département fédérale des affaires étrangères : http://www.eda.admin.ch/eda/fr/home/reps.html

4.2.2.1.4 DFPJ - Département fédéral de justice et police

Département fédéral de justice et police : http://www.ejpd.admin.ch/ejpd/fr/home.html

4.2.2.1.5 Fedpol - Lutte de la confédération contre la criminalité

Fedpol. http://www.fedpol.admin.ch/content/fedpol/fr/home.html

Selon le Fedpol, "Par cybercriminalité, on entend les infractions commises sur Internet ou directement basées sur les technologies liées au réseau Internet. Quelques exemples: les escroqueries dans les ventes aux enchères pratiquées sur Internet, le vol de données d'accès à des services sur Internet (l'hameçonnage) ou encore les attaques de hackers pénalement punissables perpétrées contre des serveurs reliés à Internet (piratage ou attaque par déni de service). Par ailleurs, la cybercriminalité englobe les infractions utilisant Internet comme moyen de communication et de coordination, par exemple pour la diffusion de pornographie enfantine."

Lutte de la confédération contre la criminalité. Page 34 :
http://www.fedpol.admin.ch/content/dam/data/sicherheit/jahresberichte/jabe-2012-f.pdf

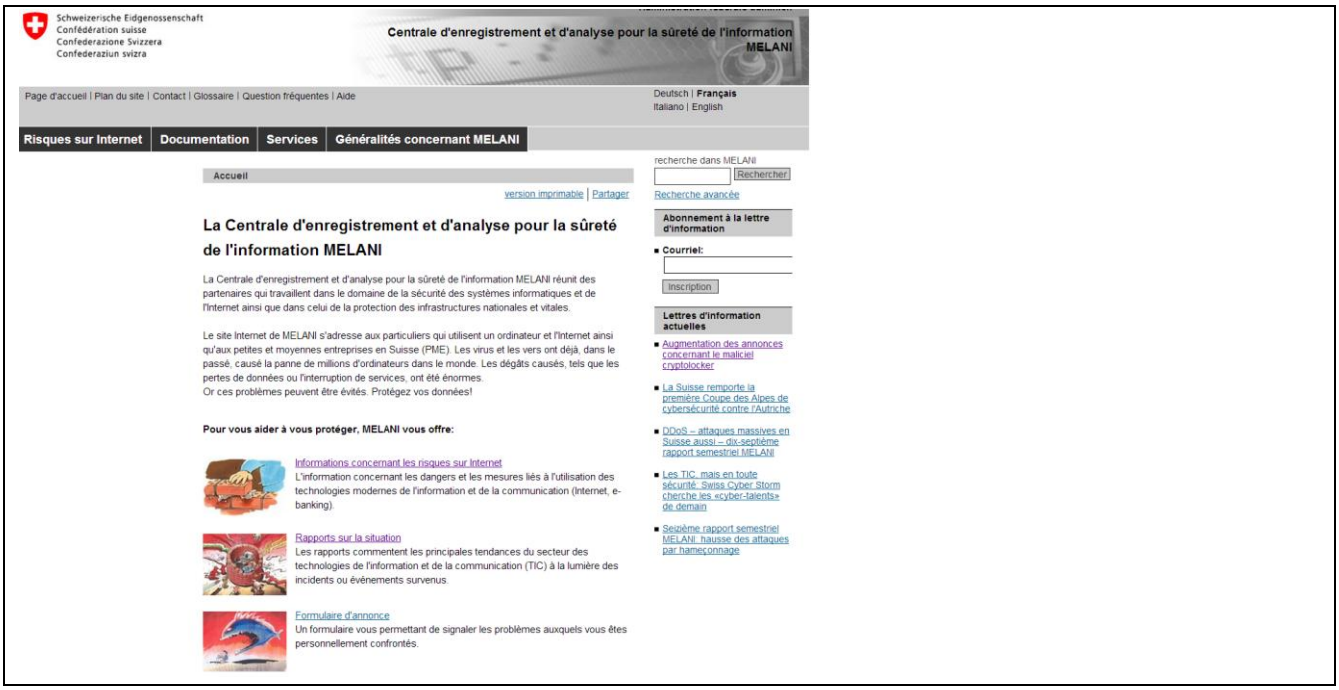
Selon ce même rapport, la criminalité basée sur l'Internet est en augmentation dans les domaines suivants :

- *Attaques contre la personnalité (la victime se montre dans une situation intime)*
- *Infractions économiques sur Internet (fausse promesse de gain, arnaques lors des enchères)*

- *Hameçonnage (Se procurer des informations de connexion à des services Internet)*
- *Réseaux privés virtuels et anonymat (transmission rapide et invisible du savoir et la coordination des actes délictueux via Skype, TOR)*
- *Connexion mobile (Infection, attaque, et vol de données des mobiles)*
- *Pornographie enfantine*

4.2.2.1.6 MELANI - Centrale d'enregistrement et d'analyse pour la sûreté de l'information.

MELANI. Centrale d'enregistrement et d'analyse pour la sûreté de l'information : http://www.melani.admin.ch/?lang=fr



Sur le site de MELANI, on trouve aussi la stratégie nationale de protection de la Suisse contre les cyberrisques.

Stratégie nationale de protection de la Suisse contre les cyberrisques : http://www.melani.admin.ch/dokumentation/00123/01525/index.html?lang=fr

4.2.2.1.7 OFCOM - Office fédéral de communications

OFCOM - Office fédéral de communications : http://www.bakom.admin.ch/index.html?lang=fr

Outil de recherche de la confédération. Critère de recherche : TIC -> http://www.bakom.admin.ch/suchen/index.html?keywords=TIC&go_search=Rechercher&lang=fr&site_mode=intern&nsb_mode=yes&search_mode=AND#volltextsuche

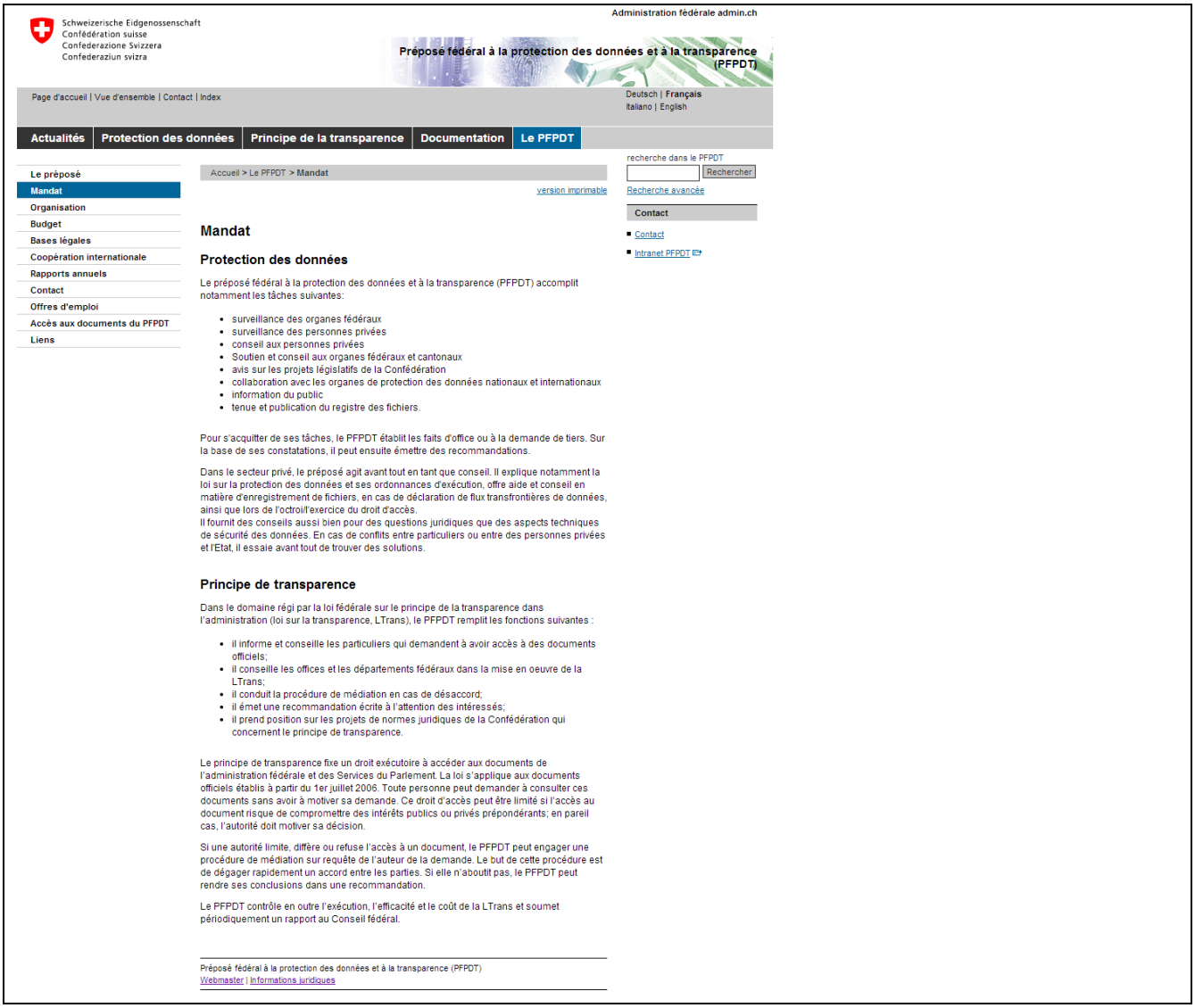
A un rôle prépondérant au niveau des TIC's car elle assure la structure permettant l'échange d'information. Pour ce qui est de la sensibilisation, l'OFCOM a développé un concept sécurité nommée "Sécurité et confiance" visant à sensibiliser la population.

4.2.2.1.8 OFJ - Office fédérale de la justice

http://www.bj.admin.ch/bj/fr/home/themen/staat_und_buerger/gesetzgebung/abgeschlossene_projekte0/datenschutz.html

4.2.2.1.9 PFPDT - Préposé fédéral à la protection des données et à la transparence

PFPDT. Préposé fédéral à la protection des données et à la transparence : http://www.edoeb.admin.ch/org/00126/index.html?lang=fr



"Le préposé fédéral à la protection des données et à la transparence (PFPDT) accomplit notamment les tâches suivantes:

- *surveillance des organes fédéraux*
- *surveillance des personnes privées*
- *conseil aux personnes privées*
- *Soutien et conseil aux organes fédéraux et cantonaux*
- *avis sur les projets législatifs de la Confédération*
- *collaboration avec les organes de protection des données nationaux et internationaux*
- *information du public*
- *tenue et publication du registre des fichiers"*

Dans le domaine régi par la loi fédérale sur le principe de la transparence dans l'administration (loi sur la transparence, LTrans)

LTrans. Loi sur la transparence : admin.ch/opc/fr/federal-gazette/2004/6807.pdf

Le préposé fédéral soumet à l'état un rapport d'activité annuel. Il permet de comprendre le périmètre d'action du préposé et son action sur la protection des données.

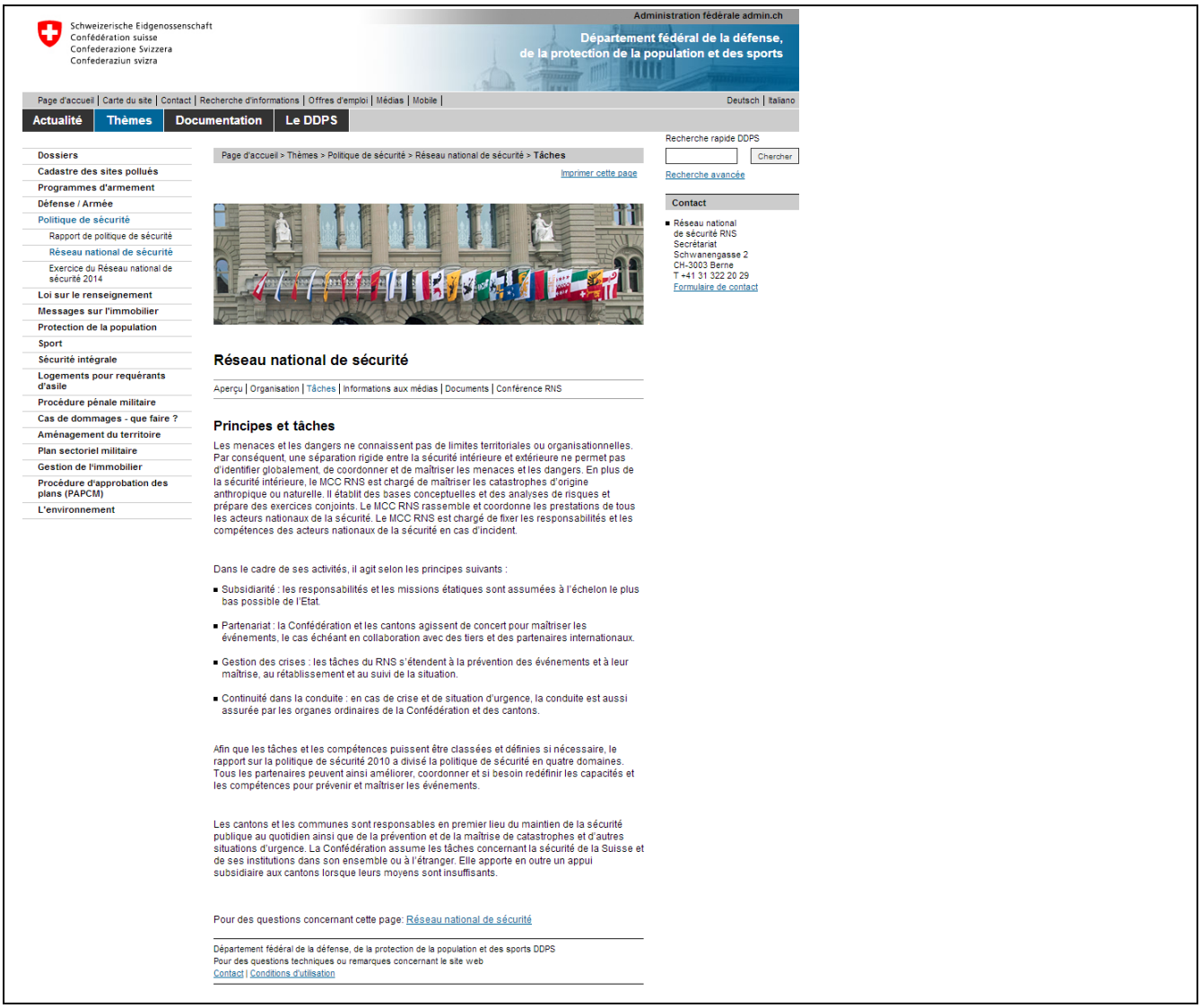
PFPDT. Préposé fédéral à la protection des données et à la transparence : http://www.edoeb.admin.ch/dokumentation/00153/01073/index.html?lang=fr

4.2.2.1.10 PJF - Police judiciaire fédérale

http://www.fedpol.admin.ch/fedpol/fr/home/fedpol/organisation/bundeskriminalpolizei.html

4.2.2.1.11 RNS - Réseau national de sécurité

http://www.vbs.admin.ch/internet/vbs/fr/home/themen/security/svs/aufgaben.html



4.2.2.1.12 SCOCI - Service national de Coordination de la lutte contre la Criminalité sur Internet

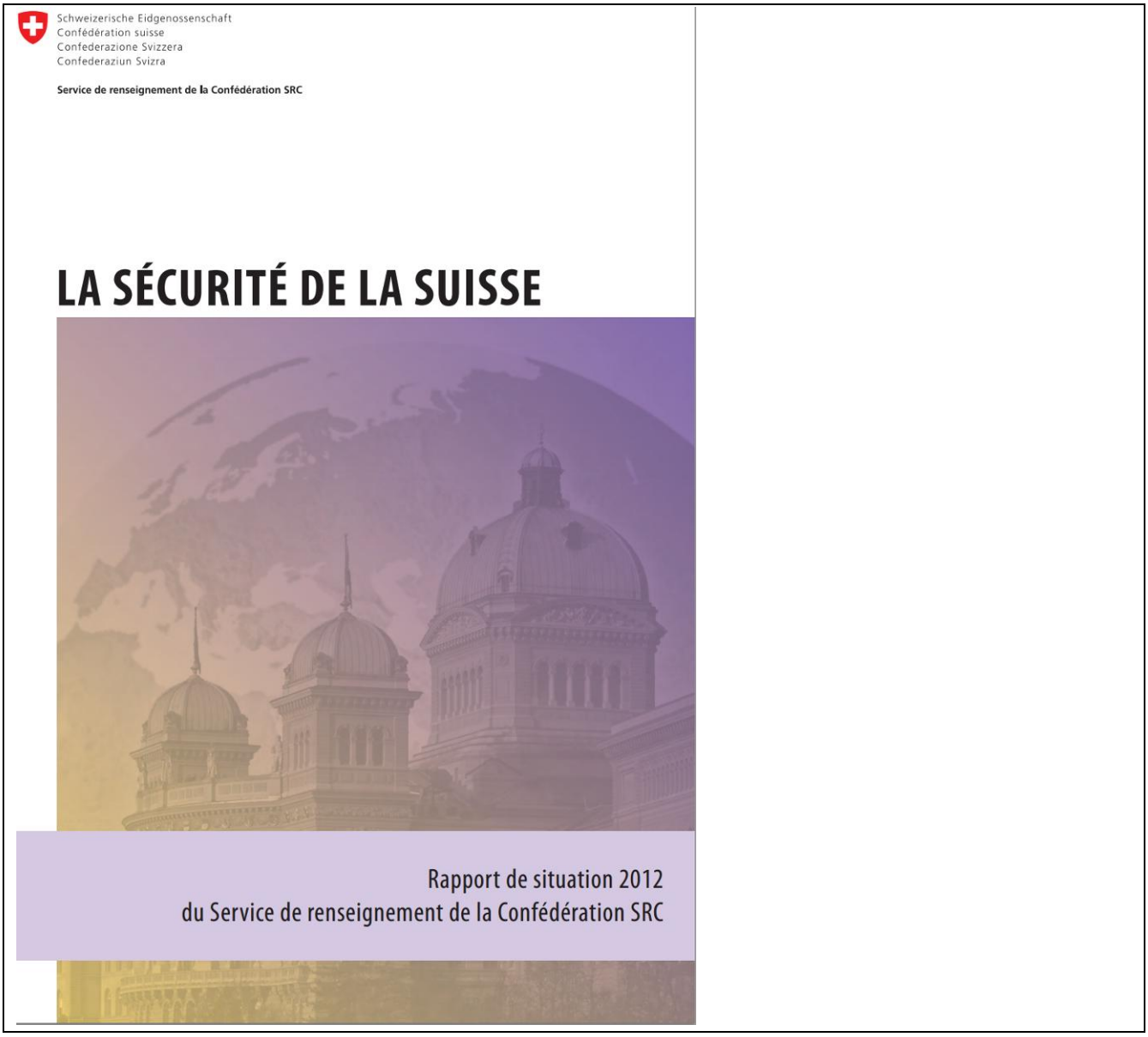
http://www.cybercrime.admin.ch/kobik/fr/home.html

4.2.2.1.13 SRC - Service de renseignement de la Confédération

Voir le(s) document(s): ndbsicherheitschweiz2012f.pdf

SRC - Service de renseignement de la Confédération

http://www.vbs.admin.ch/internet/vbs/fr/home/documentation/publication/snd_publ.parsys.75510.downloadList.74477.DownloadFile.tmp/ndbsicherheitschweiz2012f.pdf



En mai 2012, un cas de tentative de vol classifié. Un collaborateur du Service de renseignement de la Confédération (SRC) a copié des données classifiées et tenté de les vendre.

DDPS. Service de renseignement de la Confédération :
http://www.vbs.admin.ch/internet/vbs/fr/home/documentation/publication/snd_publ.html

Fuite de données déjouée :
http://www.vbs.admin.ch/internet/vbs/fr/home/documentation/publication/snd_publ.parsys.41131.downloadList.73830.DownloadFile.tmp/berichtndbf.pdf

4.2.2.1.14 SFS. Service fédéral de sécurité

http://www.fedpol.admin.ch/content/fedpol/fr/home/fedpol/organisation/bundessicherheitsdienst.html

Dans la gestion du risque, la Sécurité est l'approche permettant de prévenir les actes involontaires, tels les accidents, les erreurs de manipulation.

Il existe un Service fédéral de sécurité nommé SFS

SFS. Service fédéral de sécurité :
http://www.fedpol.admin.ch/content/fedpol/fr/home/fedpol/organisation/bundessicherheitsdienst.html

qui dépend de l'Office fédérale de la police Fedpol :

Fedpol. Office fédérale de la police :
http://www.fedpol.admin.ch/fedpol/fr/home/fedpol/organisation/bundessicherheitsdienst.html

Ce service assume les tâches de police, et structuré en trois divisions :

"Sécurité des personnes. En collaboration avec les cantons, le SFS est responsable des mesures de sécurité destinées aux personnalités de la Confédération nécessitant une protection (magistrats, parlementaires, employés de la Confédération) et aux personnes jouissant d'une protection en vertu du droit international public (par ex. chefs d'Etat, ministres, membres de familles royales). Il est chargé du recrutement, de la formation et des interventions du personnel assurant la sécurité à bord des aéronefs suisses dans le trafic aérien international et dans certains aéroports à l'étranger.

Sécurité des bâtiments. En collaboration avec les autorités cantonales, le SFS veille à la protection des bâtiments de la Confédération et des bâtiments nécessitant une protection en vertu du droit international public. Il élabore des concepts de sécurité d'ordre architectonique, technique et organisationnel destinés aux immeubles civils de la Confédération, aux domiciles privés des conseillers fédéraux, aux biens immobiliers des employés de la Confédération exposés à des risques, ainsi qu'aux représentations suisses à l'étranger (ambassades et consulats).

Centrale d'alarme. A l'aide du personnel de sécurité opérationnel, le SFS gère le Centre d'audition, assure la sécurité dans le Palais du Parlement et effectue les contrôles d'accès aux bâtiments de la Confédération. Il exploite également la centrale d'alarme de l'administration fédérale, qui reçoit en situation d'urgence les signaux d'alerte en cas d'attaque à main armée, de cambriolage ou d'incendie, ainsi que les signaux provenant d'autres systèmes d'alarme"

4.2.2.1.15 UPIC. Unité de pilotage informatique de la Confédération

L'unité de pilotage informatique de la Confédération UPIC.

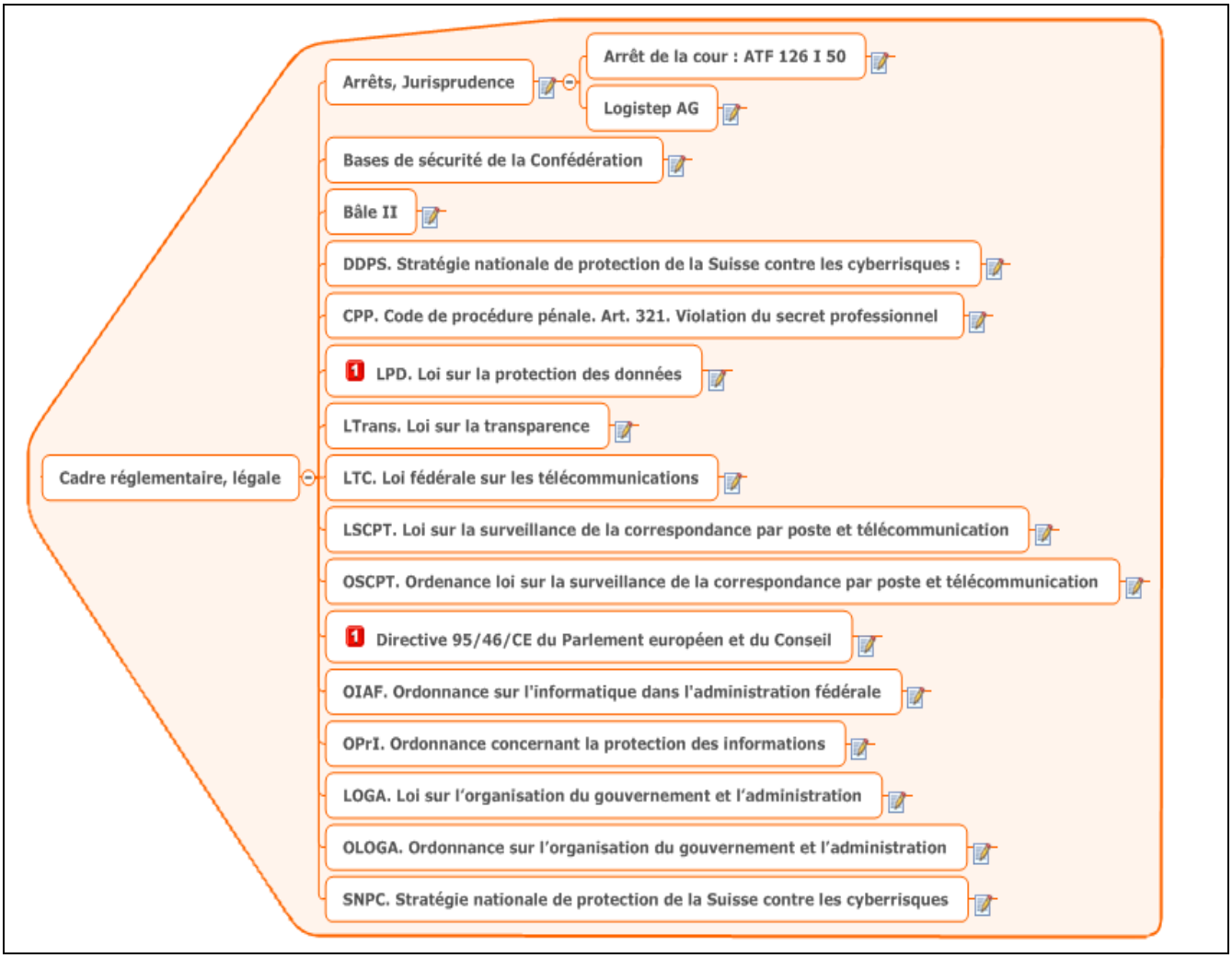
UPIC. Unité de pilotage informatique de la Confédération : http://www.isb.admin.ch/index.html?lang=fr

est chargée de mettre en oeuvre la stratégie de l'information et de la communication (TIC) du Conseil fédéral.

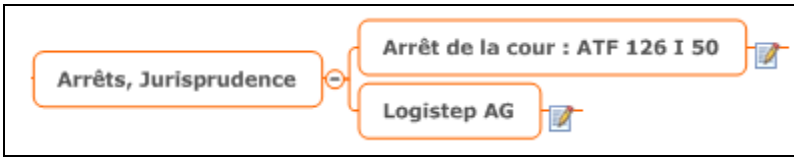
Elle édicte à cet effet des directives à l'intention des unités administratives et gère de manière centralisée les services standards en matière de TIC. Ces services sont des prestations informatiques que les unités administratives de la Confédération utilisent dans une fonctionnalité et une qualité identiques ou semblables.

L'UPIC coordonne en outre la collaboration entre la Confédération, les cantons et les communes en ce qui concerne la cyberadministration et dirige la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI.

4.2.2.2 Cadre réglementaire, légale



4.2.2.2.1 Arrêts, Jurisprudence



4.2.2.2.1.1 Arrêt de la cour : ATF 126 I 50

http://www.bger.ch/fr/index/juridiction/jurisdiction-inherit-template/jurisdiction-recht-leitentscheide1954-direct.htm

Secret des télécommunications, surveillance du courrier électronique (e-mail) ordonnée dans une procédure pénale à titre de mesure de contrainte; art. 4 aCst./art. 9 Cst., art. 36 al. 4 aCst./art. 13 al. 1 Cst., § 103 et 104 ss CPP/ZH.

Le fondement juridique des atteintes au secret des télécommunications ne se trouve pas dans la loi fédérale sur les télécommunications, mais dans les normes pertinentes de procédure pénale (consid. 2).

Est arbitraire le fait d'exiger d'un fournisseur d'accès à Internet (provider), sur la base du § 103 CPP/ZH, la recherche et l'édition de données concernant l'expéditeur et le moment de l'envoi d'un message électronique (e-mail) manipulé (consid. 4).

L'identification des participants à des conversations téléphoniques représente une atteinte au secret des télécommunications; elle doit donc satisfaire aux conditions posées à cet égard par la Constitution et par la loi (consid. 5b).

Le secret des télécommunications, garanti par la Constitution, vaut aussi pour les communications par e-mail au moyen d'Internet; exigences à respecter pour des atteintes à ce secret (consid. 6a).

La recherche et l'édition des données techniques (provenance, identification) relatives à une communication par e-mail nécessitent une base légale et doivent être approuvées par un juge (consid. 6b et 6c).

4.2.2.2.1.2 Logistep AG

L'Etat applique la protection de la sphère privée. Rares sont les cas de jurisprudence concernant la protection de la sphère privée sur territoire suisse. Cas de Logistep AG.

Logistep AG : http://www.edoeb.admin.ch/dokumentation/00153/00184/00196/index.html?lang=fr

4.2.2.2.2 Bases de sécurité de la Confédération

http://www.isb.admin.ch/themen/sicherheit/00150/index.html?lang=fr

4.2.2.2.3 Bâle II

Définissant un cadre pour la gestion du risque et de la résilience dans le secteur bancaire.

"Bâle II a entraîné une migration hors de l'évaluation simpliste le premier Accord de risques bancaires vers une approche plus holistique à travers un spectre de risques et avec un éventail de méthodes pour calculer les expositions"

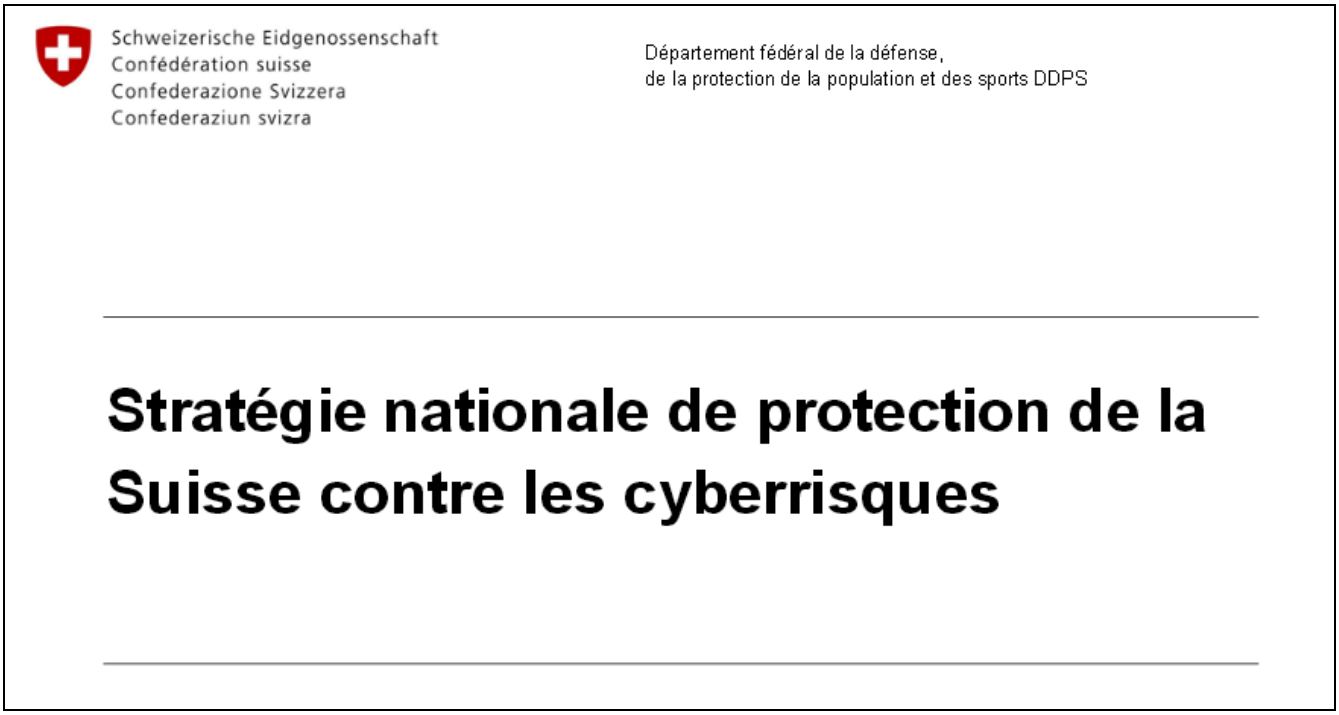
Investplus. http://www.investplus.org/contexte-impact-a02843933.htm

Le comité de Bâle définit le risque opérationnel comme le "risque de pertes provenant de processus internes inadéquats ou défaillants, de personnes et systèmes ou d'événements externes".

Dans cet ouvrage, ou recouvre les erreurs humaines, les fraudes et malveillances, les défaillances des systèmes d'information, les problèmes liés à la gestion du personnel, les litiges commerciaux, les accidents, incendies, inondations, etc.

Commission fédérale des banques http://www.finma.ch/archiv/ebk/f/internat/basel.html

4.2.2.2.4 DDPS. Stratégie nationale de protection de la Suisse contre les cyberrisques :



http://www.news.admin.ch/NSBSubscriber/message/attachments/27334.pdf

4.2.2.2.5 CPP. Code de procédure pénale. Art. 321. Violation du secret professionnel

CPP. Code de procédure pénale. Art. 321. Violation du secret professionnel

Entre autres, l'article 321 ter du Code pénal : Violation du secret professionnel.

CPP. Art. 321. Violation du secret professionnel : http://www.admin.ch/ch/f/rs/311_0/index.html

Violation du secret des postes et des télécommunications

1 Celui qui, en sa qualité de fonctionnaire, d'employé ou d'auxiliaire d'une organisation fournissant des services postaux ou de télécommunication, aura transmis à un tiers des renseignements sur les relations postales, le trafic des paiements ou les télécommunications de la clientèle, ouvert un envoi fermé ou cherché à prendre connaissance de son contenu ou encore fourni à un tiers l'occasion de se livrer à un tel acte sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

2 De même, celui qui aura déterminé par la tromperie une personne astreinte au secret en vertu de l'al. 1 à violer ce secret sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

Art. 143 du Code pénal suisse (CP). Soustraction de données :

1 Celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, aura soustrait, pour lui-même ou pour un tiers, des données enregistrées ou transmises électroniquement ou selon un mode similaire, qui ne lui étaient pas destinées et qui étaient spécialement protégées contre tout accès indu de sa part, sera puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire.

143 bis

2 La soustraction de données commise au préjudice des proches ou des familiers ne sera poursuivie que sur plainte.

1 Quiconque s'introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part est, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

2 Quiconque met en circulation ou rend accessible un mot de passe, un programme ou toute autre donnée dont il sait ou doit présumer qu'ils doivent être utilisés dans le but de commettre une infraction visée à l'al. 1 est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

Le hacking peut être considéré comme l'équivalent informatique de la violation de domicile (art. 186 CP). Avant de voler quelque chose, il faut entrer

Le système doit être « protégé contre tout accès "

http://francoischarlet.ch/2011/que-risque-le-hacker-en-droit-penal-suisse

4.2.2.2.6 LPD. Loi sur la protection des données

Voir le(s) document(s): 235.1.pdf

LPD. Loi sur la protection des données

Loi sur la protection des données. LPD. http://www.admin.ch/opc/fr/classified-compilation/19920153/201401010000/235.1.pdf

Le principe de finalité exprimé à l'art. 4 al. 3 de la loi fédérale sur la protection des données (LPD) exige que les données récoltées doivent être utilisées en conformité avec le but annoncé au moment de la collecte. La LPD n'oblige pas l'auteur du traitement à informer sur ce but, il suffit qu'il soit reconnaissable.

"Le traitement de données en question reçoive l'aval de la personne concernée sous la forme d'un consentement libre et éclairé (art. 4 al. 5 LPD)

Suivant le point de vue, la protection des données est perçue comme une protection:

1) contre le traitement abusif des données

2) du droit à l'autodétermination informationnelle

3) du droit de la personnalité dans le cadre du traitement des données

4) de la sphère privée. L'idée sur laquelle repose la protection des données est caractérisée par le droit de l'individu à décider lui-même des personnes et du moment auquel il veut rendre accessible des données personnelles déterminées. Le but de la protection des données est d'éviter l'apparition de «l'homme transparent"

Protection de données et fraude. NBI. Swiss National bureau of Insurance : http://www.nbi.ch/pdf/CC_2012_Dauphin_WS.pdf

4.2.2.2.7 LTrans. Loi sur la transparence

Loi sur la transparence. *"La présente loi vise à promouvoir la transparence quant à la mission, l'organisation et l'activité de l'administration. A cette fin, elle contribue à l'information du public en garantissant l'accès aux documents officiels."*

LTrans : Loi sur la transparence :

http://www.admin.ch/opc/fr/classified-compilation/20022540/index.html

http://www.admin.ch/opc/fr/federal-gazette/2004/6807.pdf

4.2.2.2.8 LTC. Loi fédérale sur les télécommunications

Concernant la protection des données et la sphère privée, voici quelques lois et articles qui la dessinent.

Art 2 et 3 de la loi fédérale sur les télécommunications : La LTC "règle la transmission d'informations au moyen de techniques de télécommunication, y compris la transmission de programmes de radio et de télévision"

Art. 43 Obligation d'observer le secret : "Il est interdit à toute personne qui a été ou qui est chargée d'assurer un service de télécommunication de donner à des tiers des renseignements sur les communications des usagers; de même, il lui est interdit de donner à quiconque la possibilité de communiquer de tels renseignements à des tiers"

LTC. Loi fédérale sur les télécommunications : http://www.admin.ch/ch/f/rs/784_10/index.html

4.2.2.2.9 LSCPT. Loi sur la surveillance de la correspondance par poste et télécommunication

LSCPT. Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication : http://www.admin.ch/ch/f/rs/c780_1.html

Le projet de loi révisée contient dans ses articles 31 à 34 "des règles visant à garantir le bon fonctionnement de la surveillance, imposant notamment aux fournisseurs de services de télécommunication d'être en tout temps en mesure, selon le droit applicable, de fournir des renseignements"

4.2.2.2.10 OSCPT. Ordenance loi sur la surveillance de la correspondance par poste et télécommunication

http://www.admin.ch/opc/fr/classified-compilation/20002506/201201010000/780.11.pdf

4.2.2.2.11 Directive 95/46/CE du Parlement européen et du Conseil

Voir le(s) document(s): LexUriServ.do

Directive 95/46/CE du Parlement européen et du Conseil

Cette directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données sert de cadre pour l'UE.

UE. Directive 95/46/ce du parlement européen et du conseil : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FR:HTML

4.2.2.2.12 OIAF. Ordonnance sur l'informatique dans l'administration fédérale

http://www.admin.ch/opc/fr/classified-compilation/20081009/index.html

4.2.2.2.13 OPrI. Ordonnance concernant la protection des informations

http://www.admin.ch/opc/fr/classified-compilation/20070574/index.html

4.2.2.2.14 LOGA. Loi sur l'organisation du gouvernement et l'administration

http://www.admin.ch/opc/fr/classified-compilation/19970118/index.html

La loi -et l'ordonnance- sur l'organisation du gouvernement et l'administration, s'appuyant sur l'article 173 de la constitution, structure le Département fédéral de la défense, le DDPS, via une ordonnance définissant son objectif : La défense et la protection de la population, en contribuant « à la protection de la population contre les conséquences de catastrophes, de situations d'urgence et de menaces politico-militaires ».

4.2.2.2.15 OLOGA. Ordonnance sur l'organisation du gouvernement et l'administration

http://www.admin.ch/opc/fr/classified-compilation/19983439/index.html

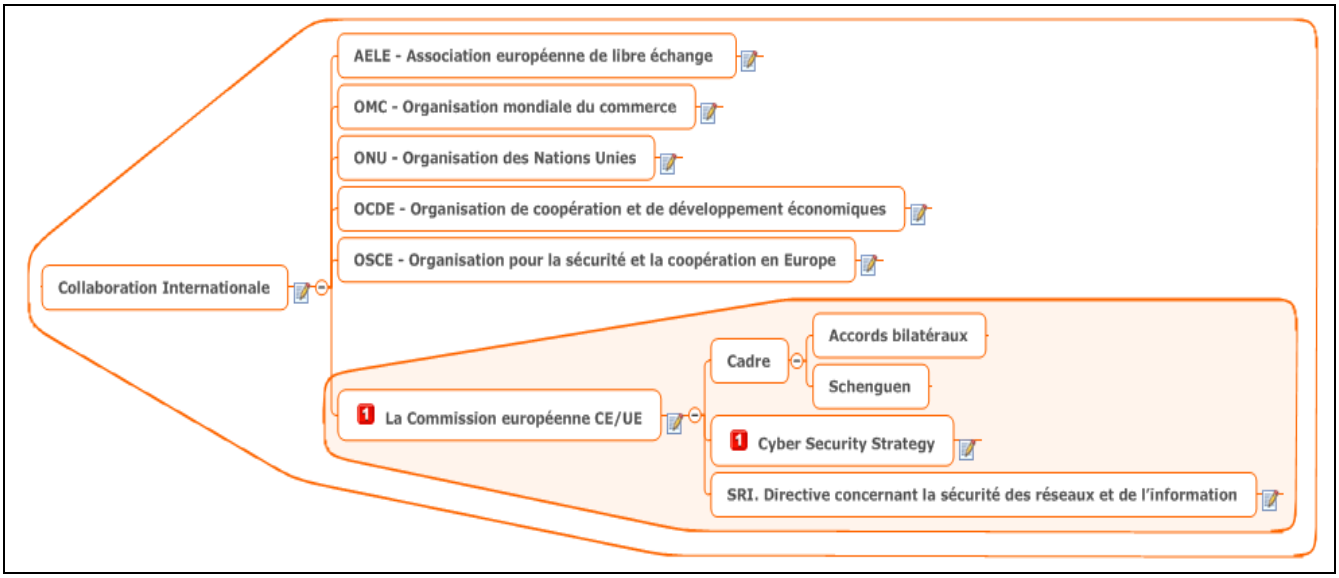
4.2.2.2.16 SNPC. Stratégie nationale de protection de la Suisse contre les cyberrisques

http://www.isb.admin.ch/themen/01709/01710/index.html?lang=fr

"Selon la stratégie, les conditions de base essentielles pour réduire les cyberrisques sont et restent la responsabilité individuelle, la collaboration au niveau national entre les milieux économiques et les autorités, ainsi que la coopération avec l'étranger. A cet effet, la stratégie prévoit 16 mesures qui devront être mises en œuvre jusqu'en 2017"

4.3 Collaboration Internationale

4.3.1 AELE - Association européenne de libre échange



http://www.seco.admin.ch/themen/00513/00515/00516/index.html?lang=fr

4.3.2 OMC - Organisation mondiale du commerce

Mission permanente de la Suisse auprès de l'Organisation mondiale du commerce OMC.

http://www.wto.org/indexfr.htm

4.3.3 ONU - Organisation des Nations Unies

Engagement de la Suisse aux Nations Unies

DFAE. Engagement de la Suisse aux Nations Unies :
http://www.eda.admin.ch/eda/fr/home/topics/intorg/un/chenun.html

4.3.4 OCDE - Organisation de coopération et de développement économiques

Voir le(s) document(s): 1326728284_FdC_GT_Normes___Certification_Livrable_v0.91.pdf, lignesdirectricesdelocderegissantlasecuritedessystemesetreseauxdinformationversuneculturedelasecurite.htm, government-at-a-glance-2013_gov_glance-2013-en

La Suisse est un des pays fondateurs de l'OCDE.

"Si beaucoup d'organisations internationales traitent de la sécurité des systèmes d'information. il existe un institut européen sur le sujet. l'OCDE tient un rôle de premier ordre. Elle a été à l'origine d'une grande part de la production de règles de sécurité et de spécifications pour les matériels et systèmes qui sont appelés les critères communs (Common Criterias). En outre, son conseil adopte des lignes directrices régissant la sécurité des systèmes et réseaux d'information"

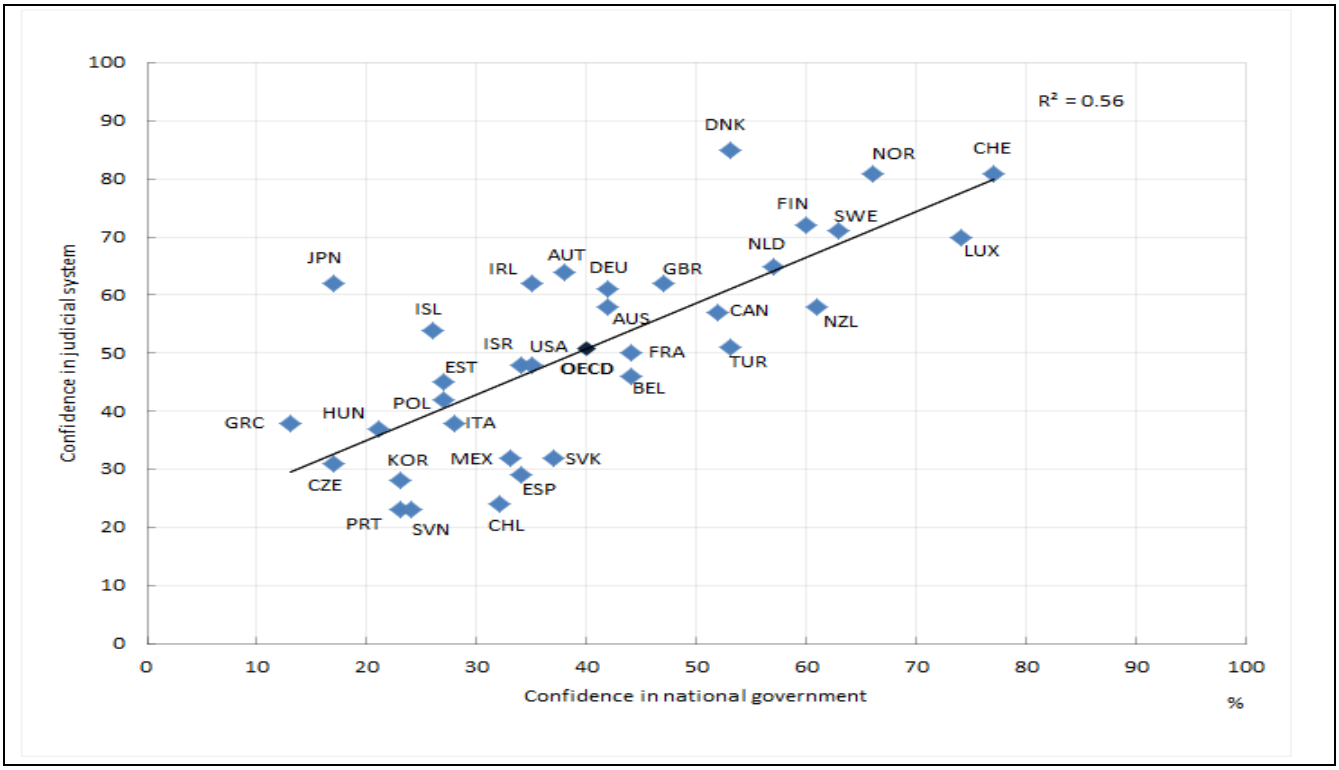
Forum des compétences, 2002, Page 22 : http://www.forum-des-competences.org/files/resourcesmodule/@random4f1443e0ce1bb/1326728284_FdC_GT_Normes___Certification_Livrable_v0.91.pdf

Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité

OCDE. Sécurité des systèmes et réseaux d'information : http://www.oecd.org/fr/internet/ieconomie/lignesdirectricesdelocderegissantlasecuritedessystemesetreseauxdinformationversuneculturedelasecurite.htm

http://www.oecd-ilibrary.org/governance/government-at-a-glance-2013_gov_glance-2013-en

1.6 Confidence in the judicial system is important for confidence in national government



4.3.5 OSCE - Organisation pour la sécurité et la coopération en Europe

Fondée en 1975 comme une conférence sur la sécurité et la coopération en Europe CSCE. Elle est constituée par 57 états.

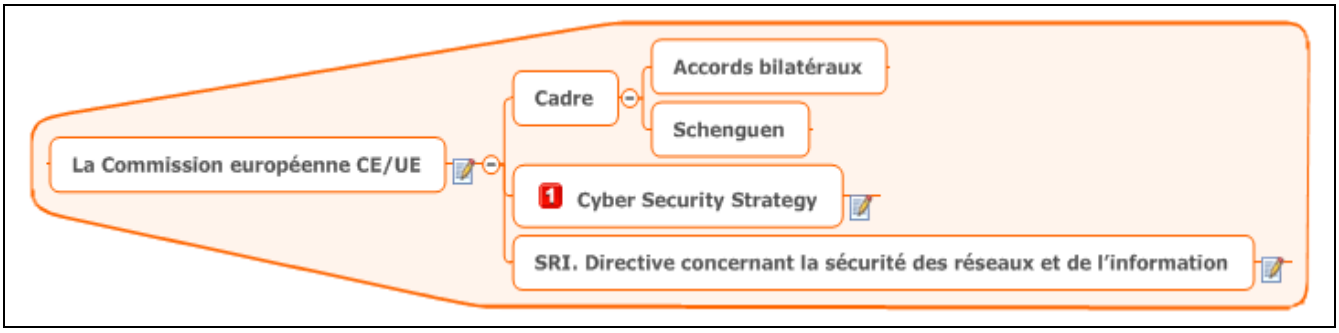
"L'OSCE est la plus grande organisation de sécurité régionale du monde. Elle œuvre en faveur de la paix, de la démocratie et de la stabilité pour plus d'un milliard de personnes. L'OSCE a une conception globale de la sécurité. Plutôt que de se limiter à la sécurité militaire traditionnelle, son action s'étend à d'autres « dimensions »: politico-militaire, économique et environnementale, humaine."

OSCE. Organization for Security and Cooperation in Europe : http://www.osce.org/

Fiche explicative

Qu'est-ce que l'OSCE? : http://www.osce.org/fr/secretariat/35779

4.3.6 La Commission européenne CE/UE



L'Office fédéral de la santé publique OFSP est responsable de la mission Suisse auprès de la commission européenne.

La Suisse et la Commission européenne mènent des discussions préliminaires afin de déterminer comment collaborer dans divers domaines.

OFSP. Office fédéral de la santé publique :
http://www.bag.admin.ch/themen/internationales/07419/index.html?lang=fr

4.3.6.1 Cadre

4.3.6.1.1 Accords bilatéraux

4.3.6.1.2 Schenguen

4.3.6.2 Cyber Security Strategy

Voir le(s) document(s): index_fr.htm, 070213_cybersecurity_fr.htm

Le 7 février 2013, l'UE propose sa stratégie en matière de cybercriminalité. Stratégie de l'UE en matière de cybersécurité : http://eeas.europa.eu/policies/eu-cyber-security/index_fr.htm

"La stratégie s'accompagne d'une proposition législative (une directive) formulée par la Commission européenne en vue de renforcer la sécurité des systèmes d'information au sein de l'Union. Cette initiative devrait promouvoir la croissance économique, dans la mesure où les citoyens se sentiront davantage en confiance lors de leurs achats en ligne et lorsqu'ils utilisent Internet. a stratégie présente des priorités claires pour la politique internationale de l'UE en matière de cybersécurité"

Stratégie de cybersécurité de l'UE. Un cyberespace ouvert, sûr et sécurisé : http://eeas.europa.eu/top_stories/2013/070213_cybersecurity_fr.htm

4.3.6.3 SRI. Directive concernant la sécurité des réseaux et de l'information

La proposition de Directive sur la SRI est un volet essentiel de la stratégie globale dont l'objectif est de garantir un environnement numérique offrant des gages de sécurité et de confiance dans toute l'UE. Elle prévoit notamment les mesures suivantes:

SRI. Directive concernant la sécurité des réseaux et de l'information : http://europa.eu/rapid/press-release_IP-13-94_en.htm

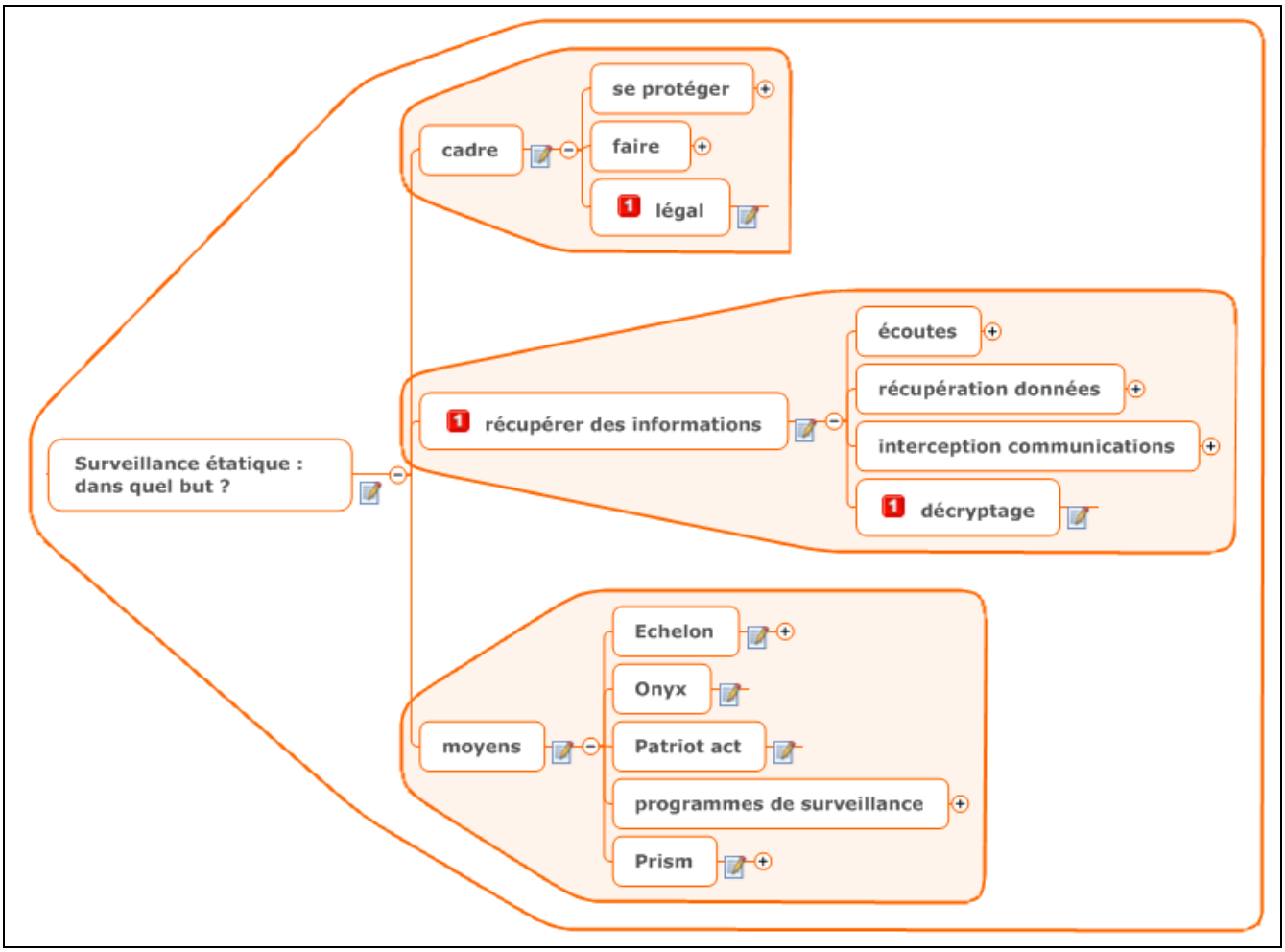
"(a) chaque Etat membre doit adopter une stratégie de SRI (art. 5) et désigner une autorité nationale compétente en la matière, qui disposera de ressources financières et humaines suffisantes pour prévenir et gérer les risques et incidents de SRI et intervenir en cas de nécessité (art. 6), ainsi que créer un centre national d'alerte et de réaction aux attaques informatiques (Computer Emergency Response Team ou « CERT ») (art. 7),

(b) un mécanisme de coopération entre les États membres et la Commission doit être instauré pour diffuser des messages d'alerte rapide sur les risques et incidents au moyen d'une infrastructure sécurisée, pour collaborer et organiser des examens par les pairs (art. 8ss),

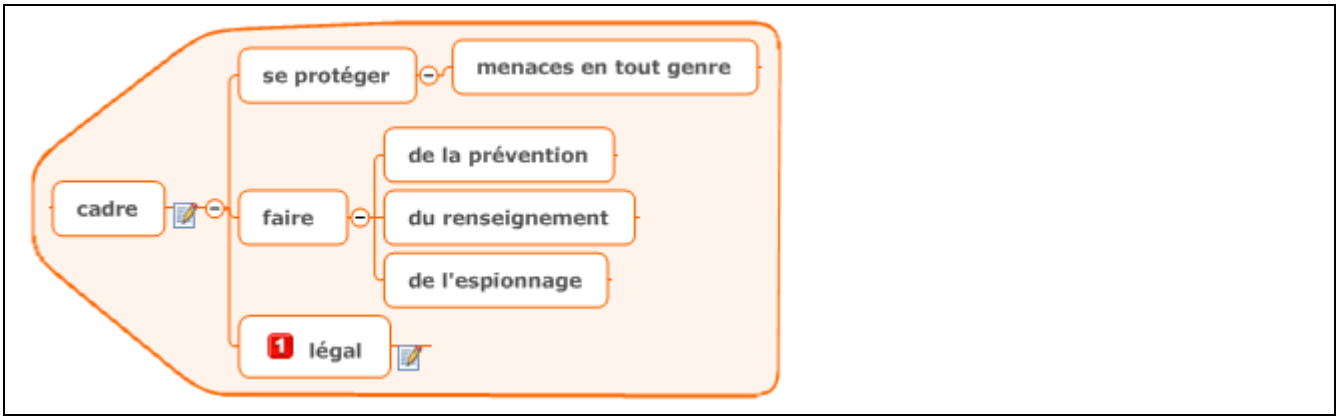
(c) les opérateurs des infrastructures critiques (services financiers, transports, énergie et santé) et les entreprises clés de l'Internet (notamment les magasins d'applications en ligne, les plates-formes de commerce électronique, les passerelles de paiement par Internet, les services informatiques en nuage, les moteurs de recherche ou les réseaux sociaux) offrant des services dans l'UE ainsi que les administrations publiques doivent adopter des pratiques en matière de gestion des risques et signaler les incidents de sécurité significatifs à l'autorité nationale (art 14)"

CERT. Computer Emergency Response Team : http://www.cert.org/

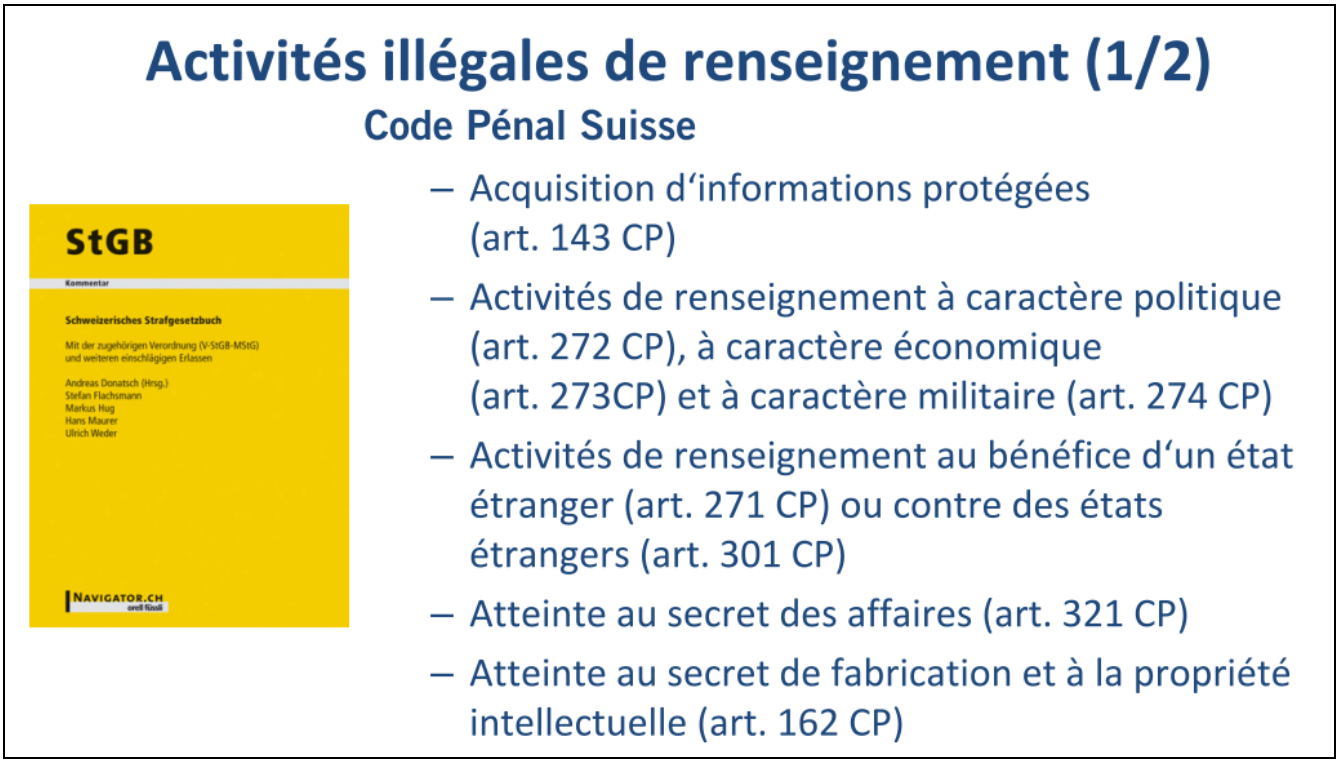
4.4 Surveillance étatique : dans quel but ?



4.4.1 cadre

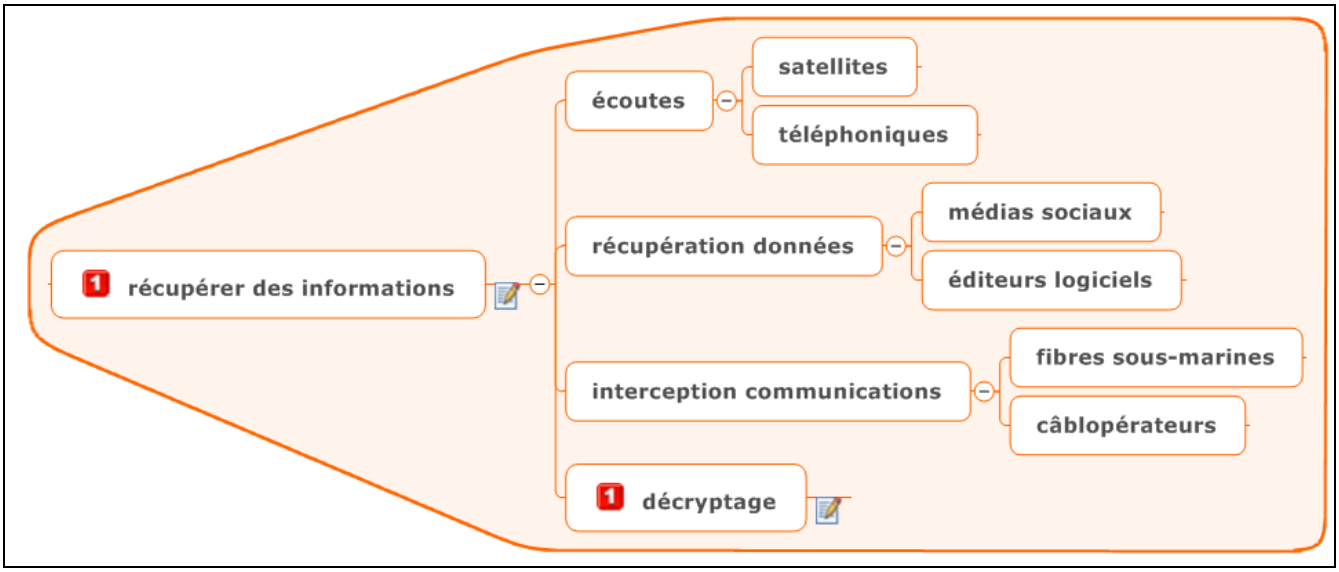


4.4.1.1 légal



©J.Pierre Therre - Formation Infosec- Module 10, Intelligence économique (2012)

4.4.2 récupérer des informations



https://www.gammagroup.com/

http://www.wikileaks.org/spyfiles/docs/GAMMA-2011-NewsQ1-en.pdf

GAMMA
GROUP INTERNATIONAL

GAMMA
NEWSLETTER Q1/2011

STRATEGIC COMMUNICATIONS MONITORING SOLUTIONS

IP MONITORING

FinLI is a Front-End system to capture IP data from IP networks according to the requirements of Lawful Interception (LI) or Intelligence Monitoring (IM). It provides the captured IP data to the Law Enforcement Monitoring Facilities (LEMF) – Monitoring Center – according to several international standards like ETSI and CALEA (and some other formats).

http://www.nouvo.ch/2013/09/gamma-finfisher-cybersurveillance-suisse-exclusif

Cybersurveillance: le sulfureux Gamma Group s'active en Suisse

EXCLUSIF La multinationale Gamma tente d'exporter ses logiciels espions depuis la Suisse. Une ONG, qui l'accuse de travailler pour des régimes autoritaires, interpelle la Confédération.

La société anglaise **Gamma Group**, qui commercialise du matériel d'écoute et des **logiciels espions** à destination des services de renseignement du monde entier, se retrouve à nouveau sous le feu des critiques.

L'ONG **Privacy International** a écrit à 70 parlementaires suisses et au Secrétariat d'Etat à l'économie (SECO), pour demander que soient refusées les demandes d'autorisation d'exportation récemment faites par Gamma Group.

Selon les informations de la RTS, ces demandes auraient été lancées via la nouvelle représentation de Gamma Group en Suisse: la filiale **Gamma Sales AG**, domiciliée depuis juin 2013 à Ittigen dans le canton de Berne.

http://www.rts.ch/video/info/journal-19h30/5213480-la-nsa-aurait-passe-un-accord-avec-les-services-secrets-suisses-pour-avoir-un-acces-direct-a-certaines-donnees.html

4.4.2.1 décryptage

http://rue89.nouvelobs.com/2014/04/14/heartbleed-nsa-aurait-exploite-plus-gros-bug-dinternet-pendant-2-ans-251473

http://mashable.com/2013/09/05/snowden-nsa-break-internet-encryption/

http://www.theguardian.com/world/interactive/2013/sep/05/sigint-nsa-collaborates-technology-companies

(U) COMPUTER NETWORK OPERATIONS
(U) SIGINT ENABLING

This Exhibit is SECRET//NOFORN									
	FY 2011[1] Actual	FY 2012 Enacted			FY 2013 Request			FY 2012 — FY 2013	
		Base	OCO	Total	Base	OCO	Total	Change	% Change
Funding ($M)	298.6	275.4	—	275.4	254.9	—	254.9	-20.4	-7
Civilian FTE	144	143	—	143	141	—	141	-2	-1
Civilian Positions	144	143	—	143	141	—	141	-2	-1
Military Positions	—	—	—	—	—	—	—	—	—

[1]Includes enacted OCO funding. Totals may not add due to rounding.

(U) Project Description

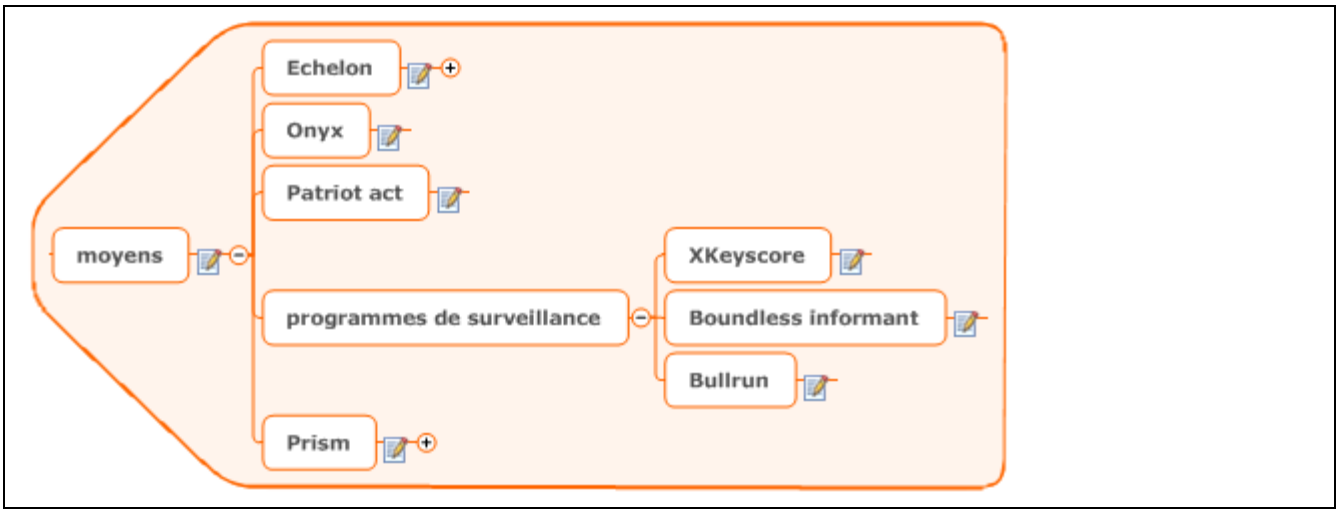
(TS//SI//NF) The SIGINT Enabling Project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable through SIGINT collection (e.g., Endpoint, MidPoint, etc.) with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact. In this way, the SIGINT Enabling approach uses commercial technology and insight to manage the increasing cost and technical challenges of discovering and successfully exploiting systems of interest within the ever-more integrated and security-focused global communications environment.

(TS//SI//REL TO USA, FVEY) This Project supports the Comprehensive National Cybersecurity Initiative (CNCI) by investing in corporate partnerships and providing new access to intelligence sources, reducing collection and exploitation costs of existing sources', and enabling expanded network operation and intelligence exploitation to support network defense and cyber situational awareness. This Project contains the SIGINT Enabling Sub-Project.

(U) Base resources in this project are used to:

- (TS//SI//REL TO USA, FVEY) Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.
- (TS//SI//REL TO USA, FVEY) Collect target network data and metadata via cooperative network carriers and/or increased control over core networks.
- (TS//SI//REL TO USA, FVEY) Leverage commercial capabilities to remotely deliver or receive information to and from target endpoints.
- (TS//SI//REL TO USA, FVEY) Exploit foreign trusted computing platforms and technologies.
- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.
- (TS//SI//REL TO USA, FVEY) Make specific and aggressive investments to facilitate the development of a robust exploitation capability against Next-Generation Wireless (NGW) communications.
- (U//FOUO) Maintain understanding of commercial business and technology trends.
- (U//FOUO) Procure products for internal evaluation.
- (U//FOUO) Partner with industry and/or government agencies in developing technologies of strategic interest to NSA/CSS.

4.4.3 moyens



4.4.3.1 Echelon

Echelon est un nom de code utilisé pendant de nombreuses années par les services de renseignements des États-Unis pour désigner une base d'interception des satellites de télécommunications commerciaux. Par extension, le réseau Echelon désigne le système mondial d'interception des communications privées et publiques (SIGINT), élaboré par les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande dans le cadre du traité UKUSA.

http://fr.wikipedia.org/wiki/Echelon


Actualités

Tous espionnés : *Surveillance électronique planétaire*

Duncan Campbell, qui révéla l'existence d'Echelon, décrit comment, par qui et pourquoi nous sommes espionnés en permanence. Vendu au prix d'une place de cinéma (40 francs), ce livre se lit comme on regarde un film d'horreur : d'abord on a peur, puis on voit les trucages. Et à la fin, on ne sait plus très bien.

Renaud Bonnet | 01net. | le 28/02/01 à 18h20 |

http://www.01net.com/editorial/138462/tous-espionnes-surveillance-electronique-planetaire/

Le système Echelon

Avec un budget annuel de 26,7 milliards de dollars — autant que pendant la guerre froide —, les services de renseignement américains sont les mieux dotés de la planète. Des alliances stratégiques et une technologie puissante leur permettent d'espionner de manière routinière téléphone, fax et courrier électronique dans le monde entier.

par **Philippe Rivière**, juillet 1999

http://www.monde-diplomatique.fr/mav/46/RIVIERE/m1

4.4.3.1.1 alliance UKUSA

http://www.tscm.com/cseukusa.html

4.4.3.2 Onyx

http://fr.wikipedia.org/wiki/Onyx_(syst%C3%A8me_d%27espionnage)

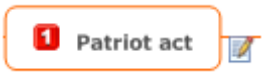
Onyx (système d'espionnage)

Pour les articles homonymes, voir Onyx.

Onyx est un système d'espionnage de satellites des services de renseignements suisses, semblable au système Echelon américain mais à une échelle beaucoup plus petite.

Originellement nommé « SATOS-3 » (les systèmes SATOS 1 et 2 ont été lancés à partir de 1992, en particulier pour intercepter les fax), Onyx est lancé en 2000 afin de surveiller des communications civiles et militaires par le biais du téléphone, du fax ou d'Internet.

4.4.3.3 Patriot act



http://www.justice.gov/archive/ll/highlights.htm

4.4.3.4 programmes de surveillance

4.4.3.4.1 XKeyscore

http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

4.4.3.4.2 Boundless informant

http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

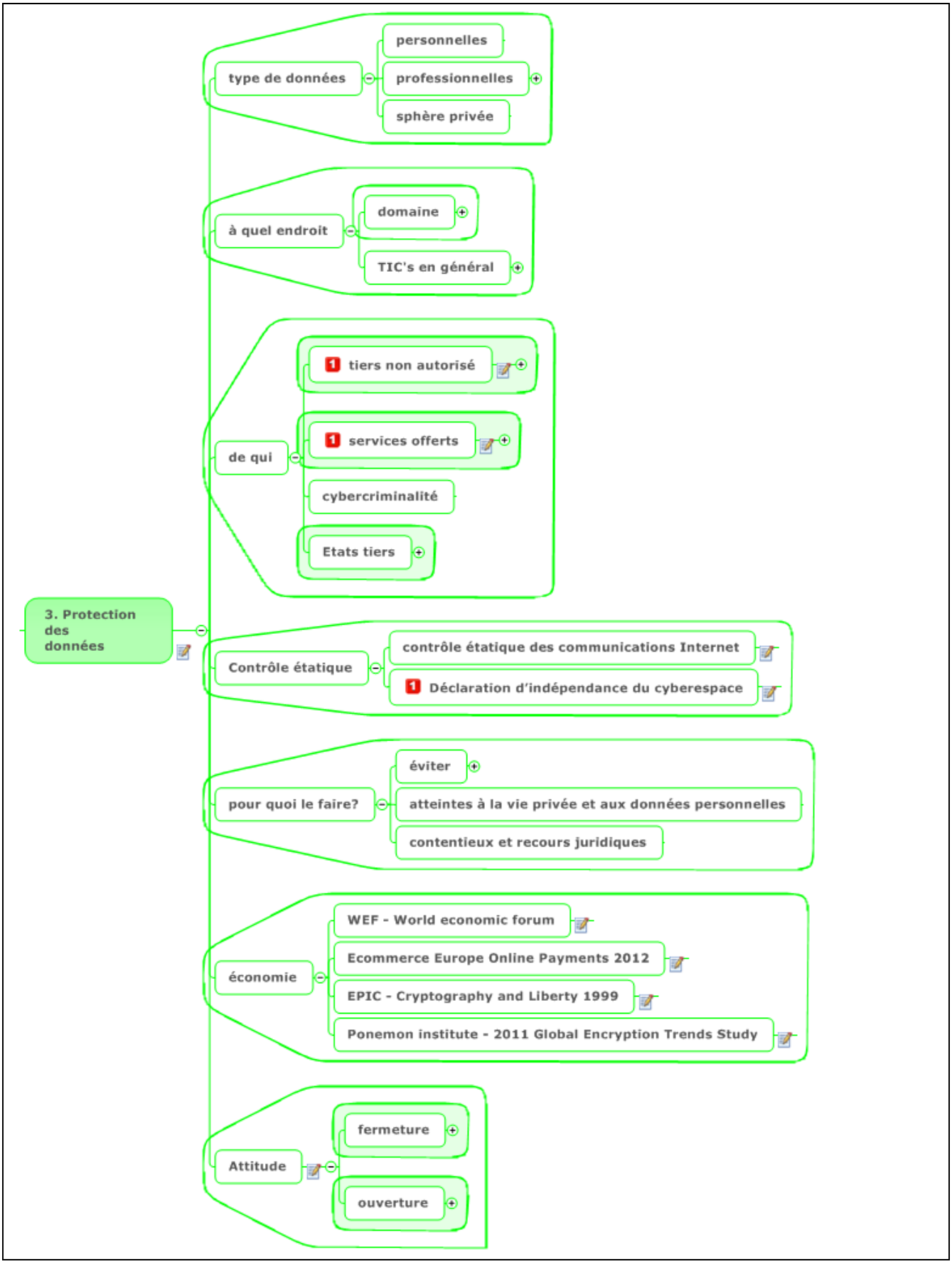
4.4.3.4.3 Bullrun

http://www.theguardian.com/world/interactive/2013/sep/05/nsa-project-bullrun-classification-guide

4.4.3.5 Prism

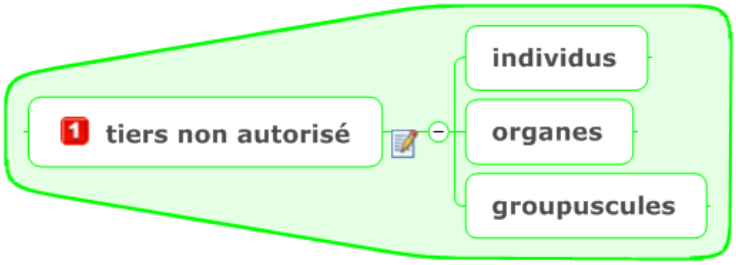
http://www.theguardian.com/world/prism

5 3. Protection des données


3. Protection des données
type de données
personnelles
professionnelles
sphère privée
à quel endroit
domaine
TIC's en général
de qui
tiers non autorisé
services offerts
cybercriminalité
Etats tiers
Contrôle étatique
contrôle étatique des communications Internet
Déclaration d'indépendance du cyberespace
pour quoi le faire?
éviter
atteintes à la vie privée et aux données personnelles
contentieux et recours juridiques
économie
WEF - World economic forum
Ecommerce Europe Online Payments 2012
EPIC - Cryptography and Liberty 1999
Ponemon institute - 2011 Global Encryption Trends Study
Attitude
fermeture
ouverture

5.1 de qui

5.1.1 2 tiers non autorisé

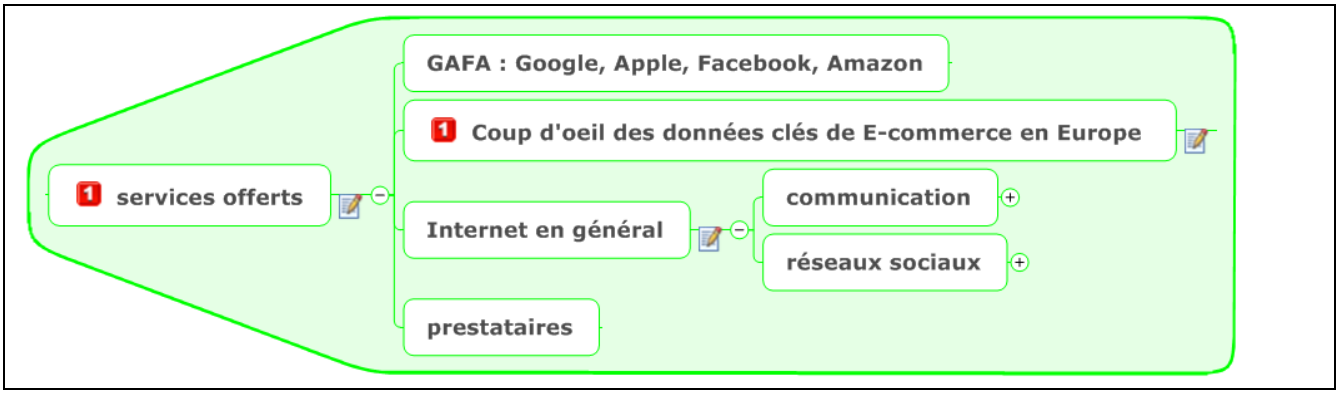


http://www.juriguide.com/les-grands-proces/20012014,herve-falciani-a-touche-mille-dollars-par-nom-de-client-hsbc-en-suisse,1176.html

http://sans-langue-de-bois.eklablog.fr/affaire-hsbc-les-zones-d-ombre-de-la-liste-falciani-le-parcours-judici-a106261382

Affaire HSBC : les zones d'ombre de la liste Falciani - Le parcours judiciaire d'une fuite bancaire sans précédent.

5.1.2 services offerts



Voir le(s) document(s): article, article

http://www.rtflash.fr/protection-donnees-personnelles-enjeu-democratique majeur/article

La vision anglo-saxonne considère au contraire que l'exportation numérique des données personnelles est devenue l'un des principaux moteurs du commerce mondial et de la croissance économique et, qu'à ce titre, elle ne doit pas faire l'objet, sauf exceptions, d'entraves ou de restrictions.

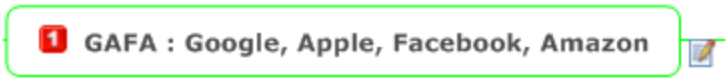
Depuis quelques mois, le projet de révision de la directive européenne sur la protection des données personnelles est entré dans une phase décisive. Ce nouveau texte vise à étendre et à améliorer la protection des informations numériques personnelles concernant les citoyens européens, lorsque celles-ci sont stockées dans des bases de données ou qu'elles circulent sur l'Internet.

Présenté début 2012 par la Commission européenne, ce projet vise à unifier et à renforcer au niveau européen le cadre de protection pour ce type de données. Concrètement, un guichet unique sera instauré : si un internaute britannique ou allemand est en conflit avec une entreprise située en Espagne, il ne sera plus obligé d'effectuer des démarches auprès de l'agence espagnole de protection des données et pourra saisir directement l'agence britannique ou allemande.

Mais le point central de ce projet de directive, celui qui suscite les débats les plus vifs entre états et provoque également une forte opposition de la part des États-Unis, est la modification de la règle du "consentement explicite". Cela signifie que ce texte prévoit d'inverser la logique actuelle : aujourd'hui, les grands du numérique peuvent utiliser vos données personnelles, sauf si vous vous y opposez expressément. Demain, si cette directive est adoptée, les géants du Net devront d'abord obtenir votre autorisation pour se servir des informations vous concernant.

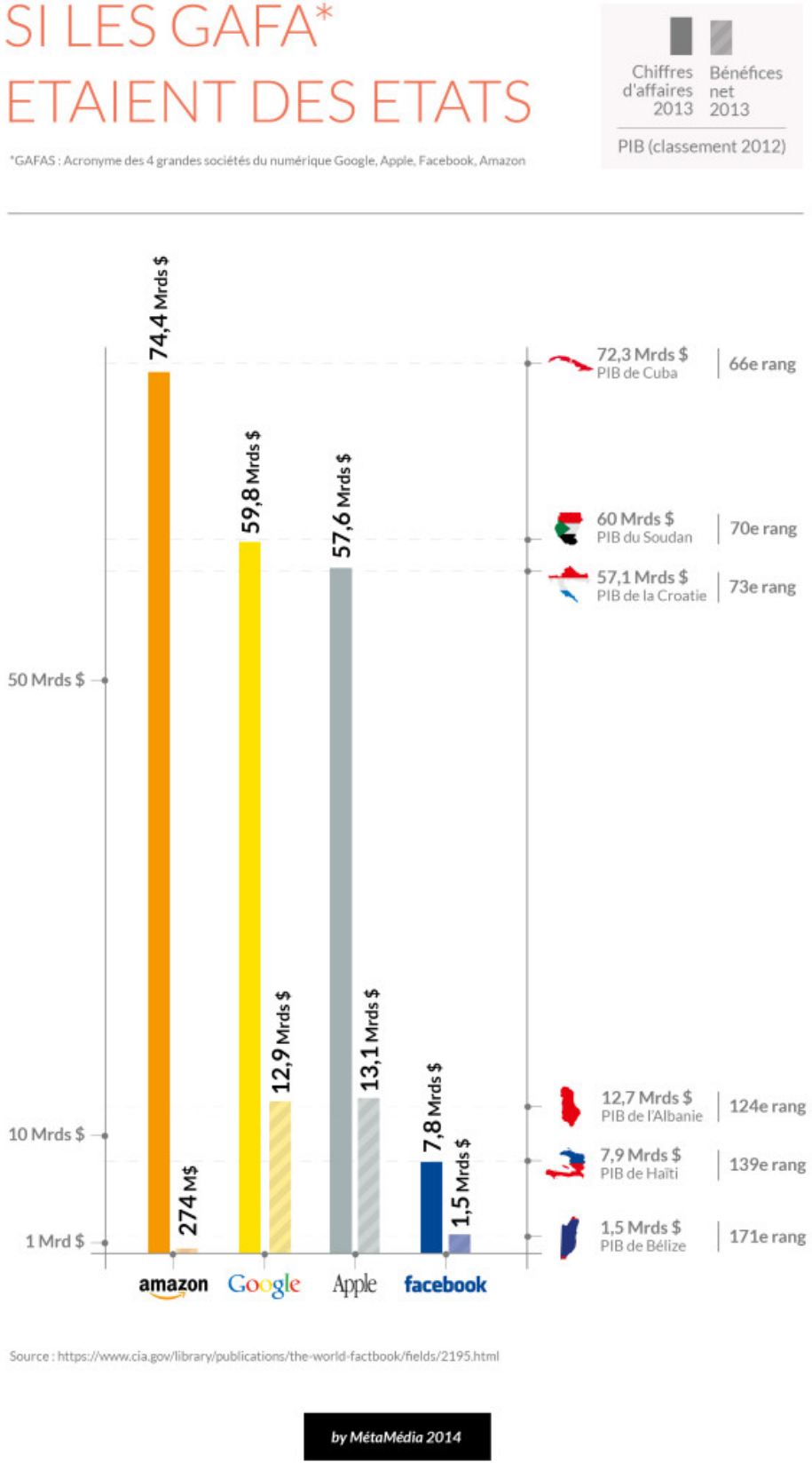
5.1.2.1 GAFA : Google, Apple, Facebook, Amazon

Voir le(s) document(s): si-les-gafa-etaient-des-etats-infographie.html



http://meta-media.fr/2014/02/07/si-les-gafa-etaient-des-etats-infographie.html

Si les GAFA étaient des Etats [infographie]



5.1.2.2 Coup d'oeil des données clés de E-commerce en Europe

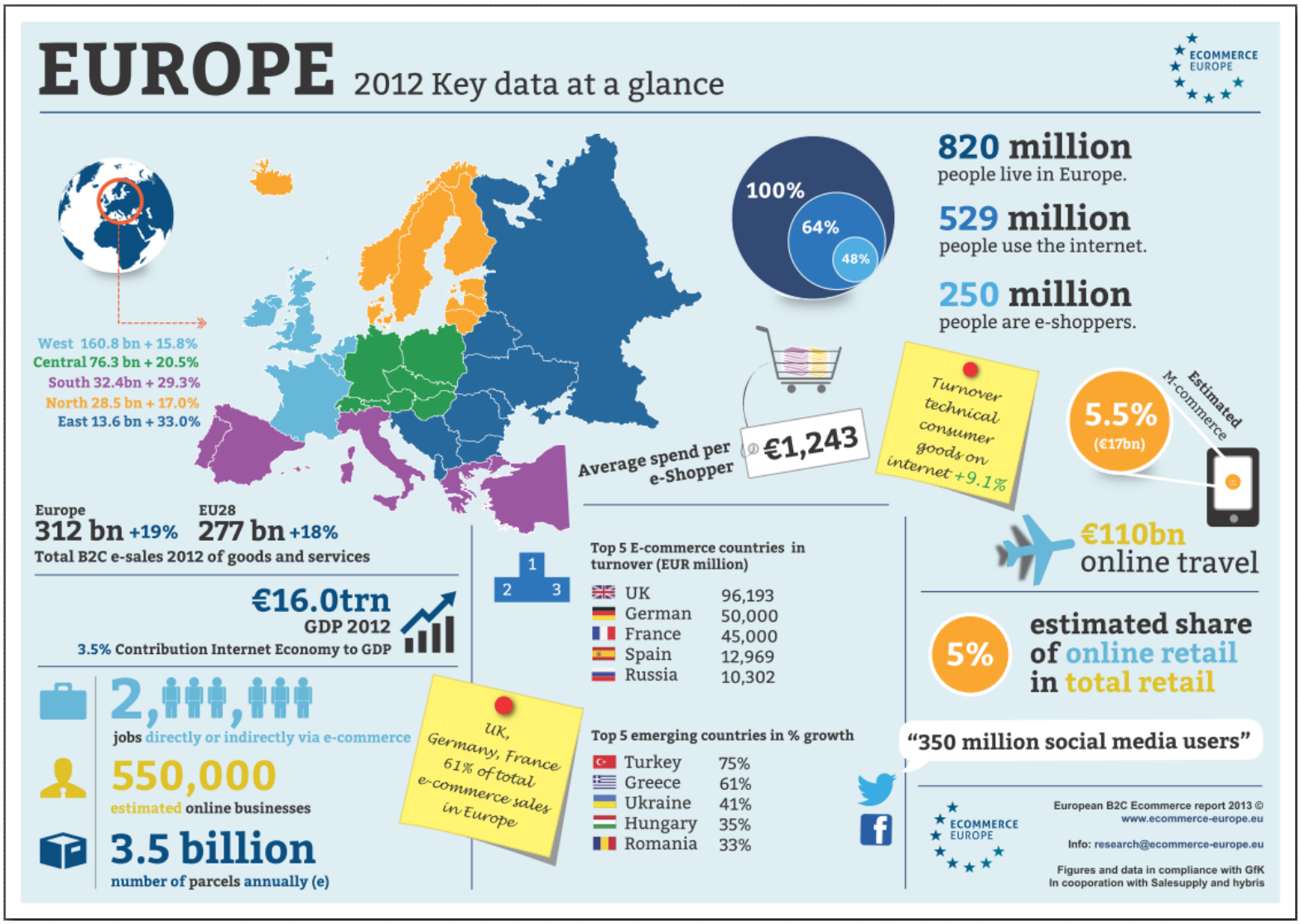
Voir le(s) document(s): infographic-europe-key-data-at-glance-2012

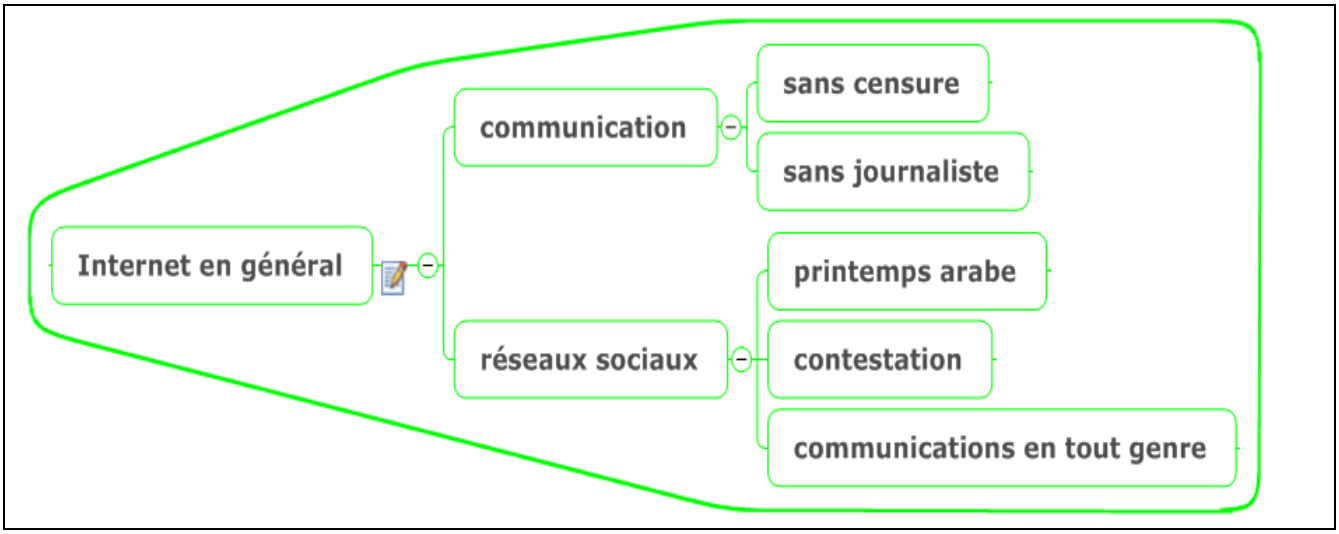
Coup d'oeil des données clés de E-commerce en Europe

http://fr.slideshare.net/meaoist/infographic-europe-key-data-at-glance-2012

http://www.retailexcellence.ie/images/uploads/downloads/members_resources/Europe_B2C_Ecommerce_Report_2013.pdf

5.1.2.3 Internet en général





5.2 Contrôle étatique

5.2.1 contrôle étatique des communications Internet

http://www.parlament.ch/e/suche/pages/geschaefte.aspx?gesch_id=20023739

5.2.2 Déclaration d'indépendance du cyberespace

Voir le(s) document(s): Declaration-Final.html, com.php

Déclaration d'indépendance du cyberespace

Original : https://projects.eff.org/~barlow/Declaration-Final.html

Traduction par le parti Pirate : https://partipirate.org/blog/com.php?id=1267

DECLARATION D'INDEPENDANCE DU CYBERESPACE (5)

Gouvernements du monde industriel, géants fatigués de chair et d'acier, je viens du cyberespace, nouvelle demeure de l'esprit. Au nom de l'avenir, je vous demande, à vous qui êtes du passé, de nous laisser tranquilles. Vous n'êtes pas les bienvenus parmi nous. Vous n'avez aucun droit de souveraineté sur nos lieux de rencontre.

Nous n'avons pas de gouvernement élu et nous ne sommes pas près d'en avoir un, aussi je m'adresse à vous avec la seule autorité que donne la liberté elle-même lorsqu'elle s'exprime. Je déclare que l'espace social global que nous construisons est indépendant, par nature, de la tyrannie que vous cherchez à nous imposer. Vous n'avez pas le droit moral de nous donner des ordres et vous ne disposez d'aucun moyen de contrainte que nous ayons de vraies raisons de craindre.

Les gouvernements tirent leur pouvoir légitime du consentement des gouvernés. Vous ne nous l'avez pas demandé et nous ne vous l'avons pas donné. Vous n'avez pas été conviés. Vous ne nous connaissez pas et vous ignorez tout de notre monde. Le cyberespace n'est pas borné par vos frontières. Ne croyez pas que vous puissiez le construire, comme s'il s'agissait d'un projet de construction publique. Vous ne le pouvez pas. C'est un acte de la nature et il se développe grâce à nos actions collectives.

Vous n'avez pas pris part à notre grande conversation, qui ne cesse de croître, et vous n'avez pas créé la richesse de nos marchés. Vous ne connaissez ni notre culture, ni notre éthique, ni les codes non écrits qui font déjà de notre société un monde plus ordonné que celui que vous pourriez obtenir en imposant toutes vos règles.

Vous prétendez que des problèmes se posent parmi nous et qu'il est nécessaire que vous les régliez. Vous utilisez ce prétexte pour envahir notre territoire. Nombre de ces problèmes n'ont aucune existence. Lorsque de véritables conflits se produiront, lorsque des erreurs seront commises, nous les identifierons et nous les réglerons par nos propres moyens. Nous établissons notre propre contrat social. L'autorité y sera définie selon les conditions de notre monde et non du vôtre. Notre monde est différent.

Le cyberespace est constitué par des échanges, des relations, et par la pensée elle-même, déployée comme une vague qui s'élève dans le réseau de nos communications. Notre monde est à la fois partout et nulle part, mais il n'est pas là où vivent les corps.

Nous créons un monde où tous peuvent entrer, sans privilège ni préjugé dicté par la race, le pouvoir économique, la puissance militaire ou le lieu de naissance.

Nous créons un monde où chacun, où qu'il se trouve, peut exprimer ses idées, aussi singulières qu'elles puissent être, sans craindre d'être réduit au silence ou à une norme.

Vos notions juridiques de propriété, d'expression, d'identité, de mouvement et de contexte ne s'appliquent pas à nous. Elles se fondent sur la matière. Ici, il n'y a pas de matière.

Nos identités n'ont pas de corps; ainsi, contrairement à vous, nous ne pouvons obtenir l'ordre par la contrainte physique. Nous croyons que l'autorité naîtra parmi nous de l'éthique, de l'intérêt individuel éclairé et du bien public. Nos identités peuvent être réparties sur un grand nombre de vos juridictions. La seule loi que toutes les cultures qui nous constituent s'accordent à reconnaître de façon générale est la Règle d'Or (6). Nous espérons que nous serons capables d'élaborer nos solutions particulières sur cette base. Mais nous ne pouvons pas accepter les solutions que vous tentez de nous imposer.

Aux États-Unis, vous avez aujourd'hui créé une loi, la loi sur la réforme des télécommunications, qui viole votre propre Constitution et représente une insulte aux rêves de Jefferson, Washington, Mill, Madison, Tocqueville et Brandeis (7). Ces rêves doivent désormais renaître en nous.

Vous êtes terrifiés par vos propres enfants, parce qu'ils sont les habitants d'un monde où vous ne serez jamais que des étrangers. Parce que vous les craignez, vous confiez la responsabilité parentale, que vous êtes trop lâches pour prendre en charge vous-mêmes, à vos bureaucraties. Dans notre monde, tous les sentiments, toutes les expressions de l'humanité, des plus vils aux plus angéliques, font partie d'un ensemble homogène, la conversation globale informatique. Nous ne pouvons pas séparer l'air qui suffoque de l'air dans lequel battent les ailes.

En Chine, en Allemagne, en France, en Russie, à Singapour, en Italie et aux États-Unis (8), vous vous efforcez de repousser le virus de la liberté en érigeant des postes de garde aux frontières du cyberespace. Ils peuvent vous préserver de la contagion pendant quelque temps, mais ils n'auront aucune efficacité dans un monde qui sera bientôt couvert de médias informatiques.

Vos industries de l'information toujours plus obsolètes voudraient se perpétuer en proposant des lois, en Amérique et ailleurs, qui prétendent définir des droits de propriété sur la parole elle-même dans le monde entier. Ces lois voudraient faire des idées un produit industriel quelconque, sans plus de noblesse qu'un morceau de fonte. Dans notre monde, tout ce que l'esprit humain est capable de créer peut être reproduit et diffusé à l'infini sans que cela ne coûte rien. La transmission globale de la pensée n'a plus besoin de vos usines pour s'accomplir.

Ces mesures toujours plus hostiles et colonialistes nous mettent dans une situation identique à celle qu'ont connue autrefois les amis de la liberté et de l'autodétermination, qui ont eu à rejeter l'autorité de pouvoirs distants et mal informés. Nous devons déclarer nos subjectivités virtuelles étrangères à votre souveraineté, même si nous continuons à consentir à ce que vous ayez le pouvoir sur nos corps. Nous nous répandrons sur la planète, si bien que personne ne pourra arrêter nos pensées.

Nous allons créer une civilisation de l'esprit dans le cyberespace. Puisse-t-elle être plus humaine et plus juste que le monde que vos gouvernements ont créé.

Davos (Suisse), le 8 février 1996.

John Perry Barlow, Cognitive Dissident Co-Founder, Electronic Frontier Foundation Home (stead) Page: http://www.eff.org /~barlow Message Service: 800/634-3542 Barlow in Meatspace Today (until Feb 12): Cannes, France Hotel Martinez: (33) 92 98 73 00, Fax: (33) 93 39 67 82 Coming soon to: Amsterdam 2/13-14, Winston-Salem 2/15, San Francisco 2/16-20, San Jose 2/21, San Francisco 2/21-23, Pinedale, Wyoming¶.

**********In Memoriam, Dr. Cynthia Horner et Jerry Garcia **********

5.2.3 atteintes à la sphère privée et aux données personnelles

5.2.4 contentieux et recours juridiques

5.3 économie

5.3.1 WEF - World economic forum

http://reports.weforum.org/hyperconnected-world-2014/wp-content/blogs.dir/37/mp/files/pages/files/final-15-01-risk-and-responsibility-in-a-hyperconnected-world-report.pdf

5.3.2 Ecommerce Europe Online Payments 2012

http://www.ecommerce-europe.eu/publications/2012/06/report-ecommerce-europe-online-payments-2012

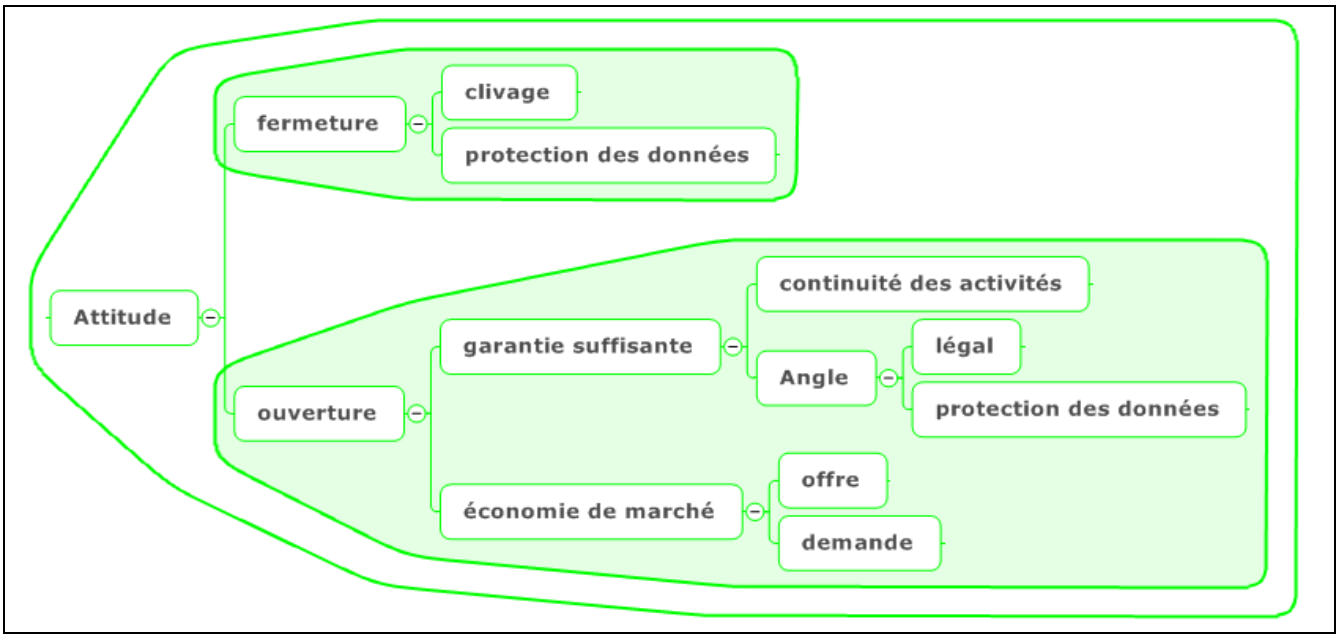
5.3.3 EPIC - Cryptography and Liberty 1999

http://gilc.org/crypto/crypto-survey-99.html#_Toc450793222

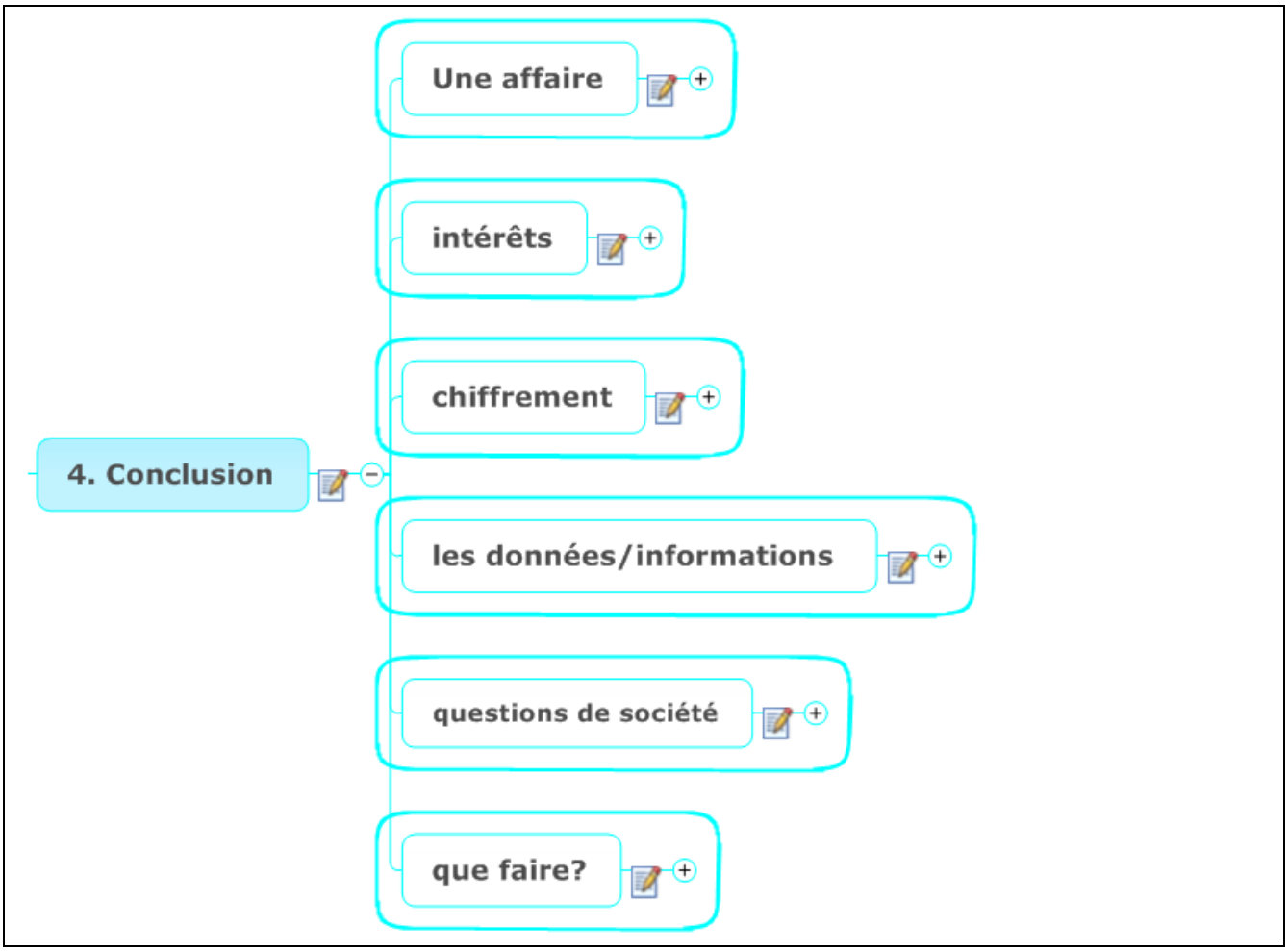
5.3.4 Ponemon institute - 2011 Global Encryption Trends Study

http://www.ponemon.org/local/upload/file/2011_Global_Encryption_Trends_Study_FINAL.pdf

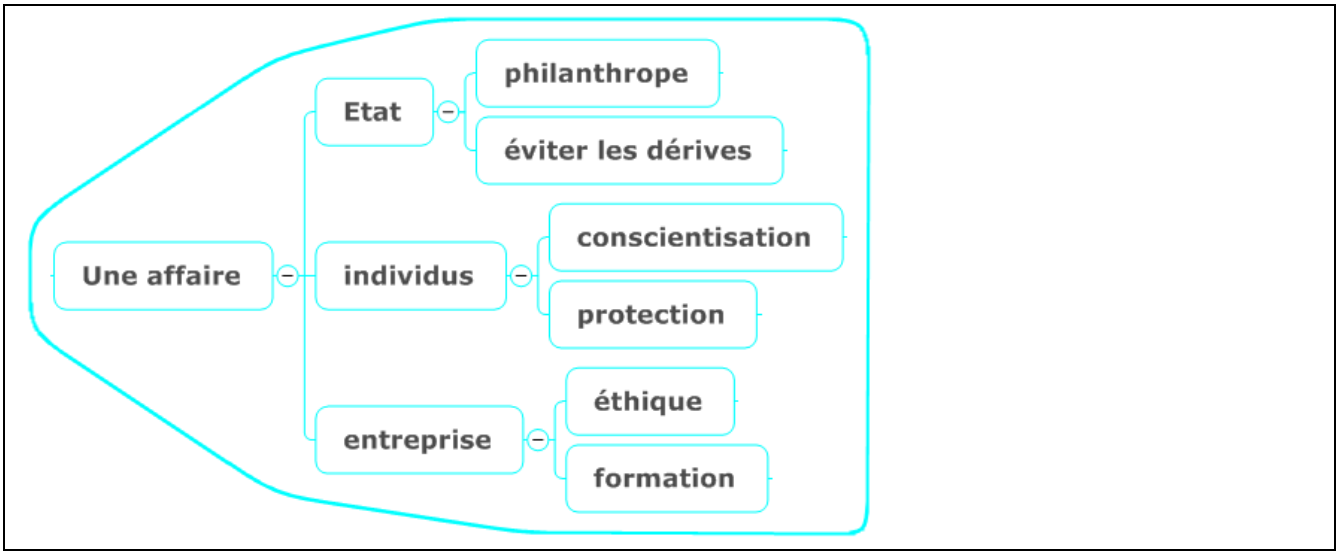
5.4 Attitude



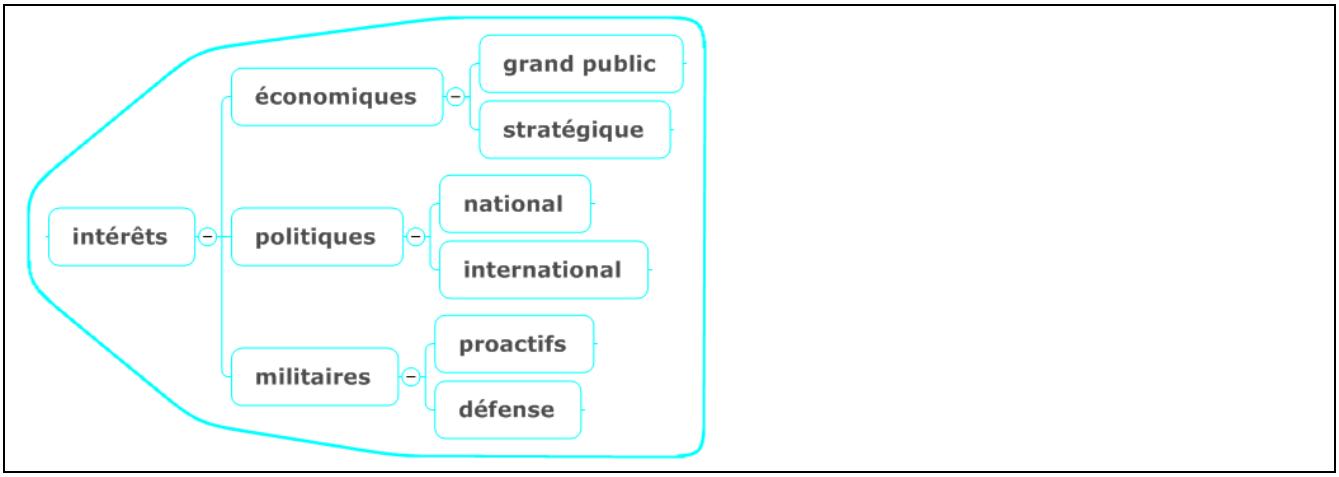
6 4. Conclusion



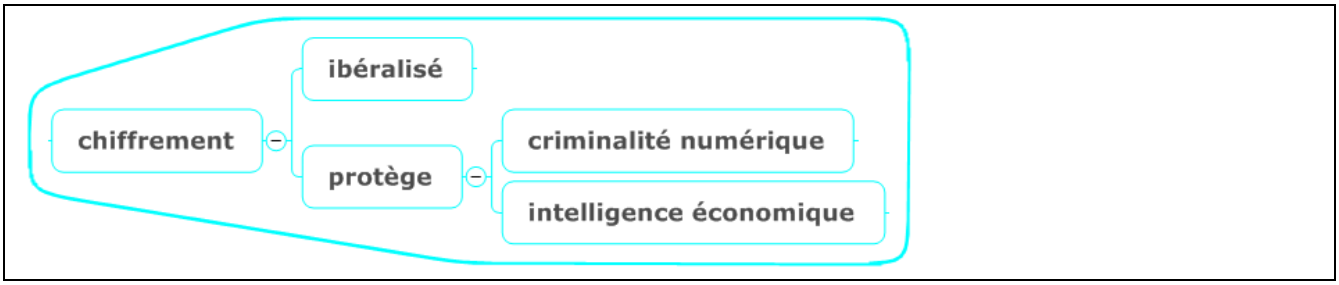
6.1 Une affaire



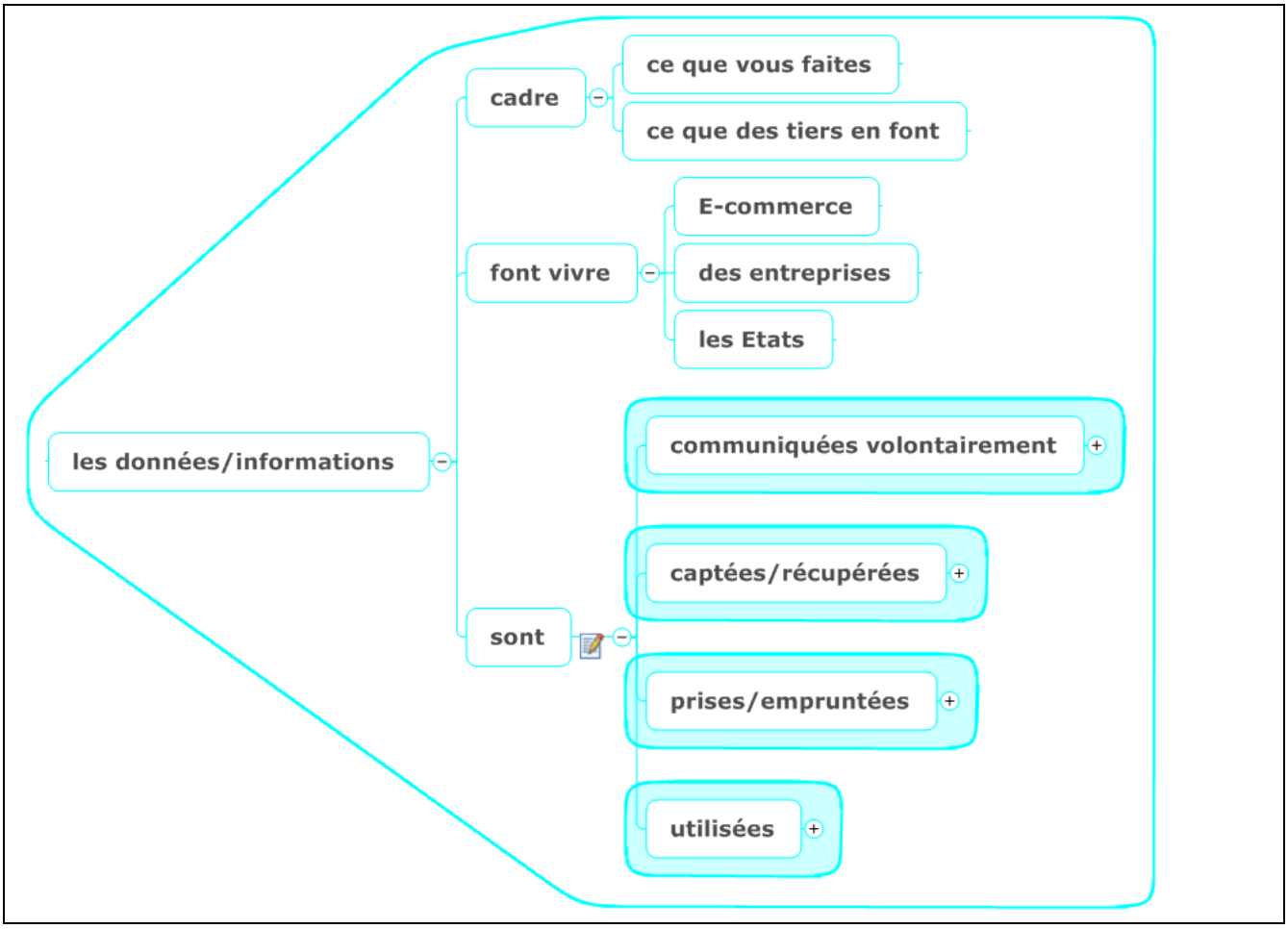
6.2 intérêts



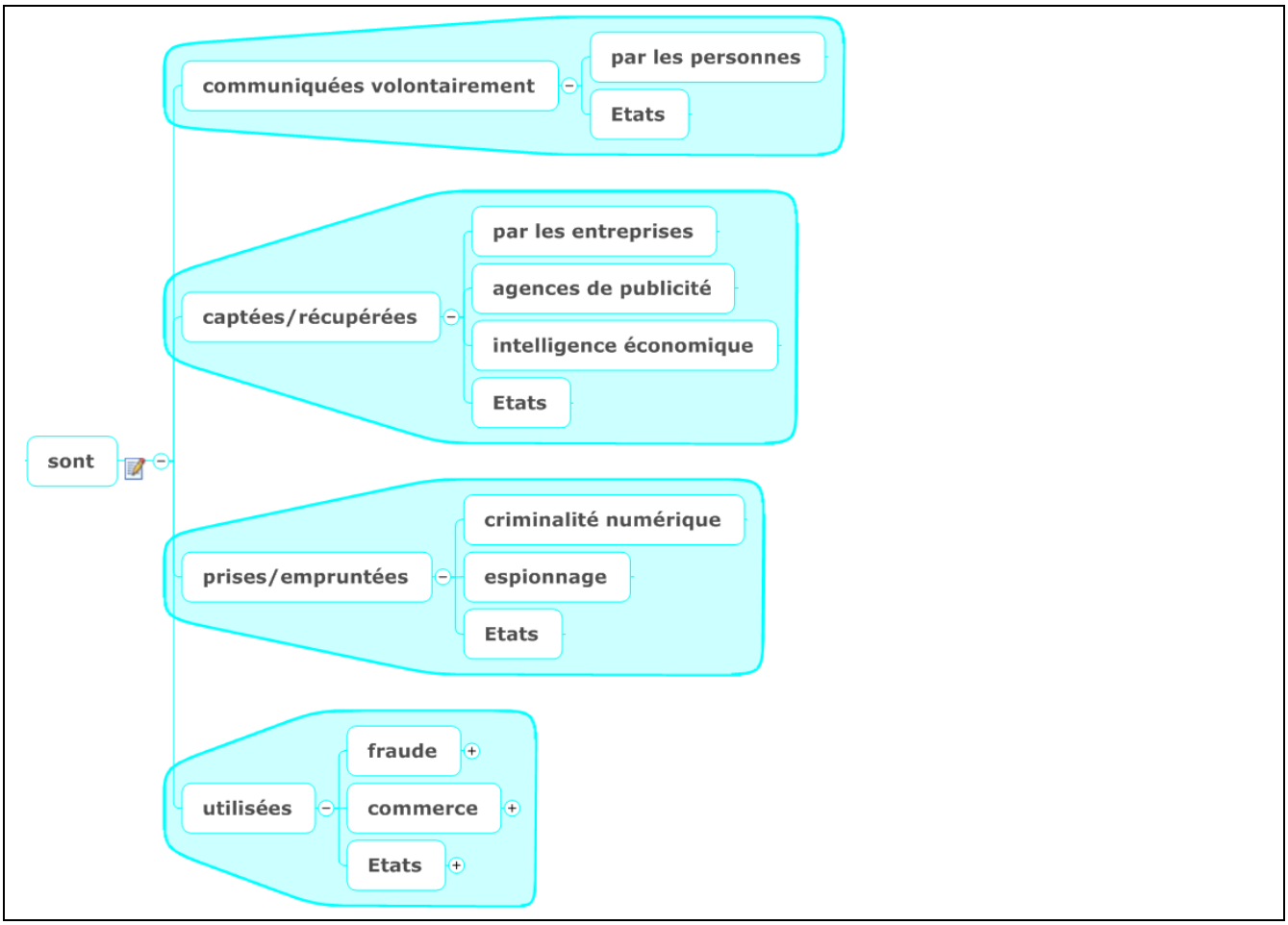
6.3 chiffrement



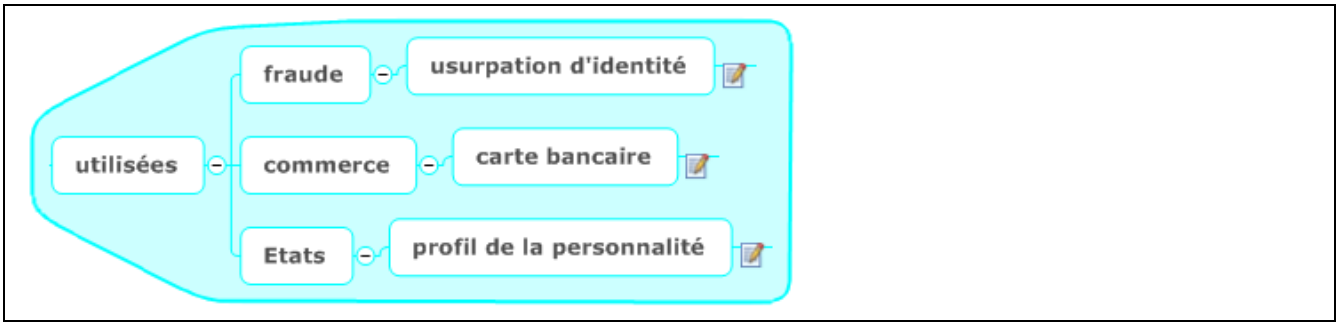
6.4 les données/informations



6.4.1 sont



6.4.1.1 utilisées



6.4.1.1.1 fraude

6.4.1.1.1.1 usurpation d'identité

Usurpation d'identité

En Suisse : http://francoischarlet.ch/2013/usurpation-didentite-le-conseil-federal-ne-legiferera-pas-et-il-a-tort

En France : http://fr.wikipedia.org/wiki/Usurpation_d'identit%C3%A9

Le populaire.fr : http://www.lepopulaire.fr/limousin/actualite/2013/02/25/cybercriminalite-120-000-victimes-d-usurpation-d-identite-chaque-annee-en-france_1456223.html

Cybercriminalité : 120.000 victimes d'usurpation d'identité chaque année en France

Lu 3462 fois 2

Daniel Martin, ancien commissaire de la DST, spécialiste des nouvelles technologies. - Brigitte Azzopard


Recommander Partager inscription pour voir ce que vos amis recommandent.

Daniel Martin, ancien commissaire de la DST, spécialisé dans les nouvelles technologies donnait une conférence à Limoges pour évoquer les différentes formes de délinquance sur le net. Etat des lieux...

Internet est un formidable outil d'ouverture sur le monde mais peut s'avérer extrêmement dangereux. C'est le propos que développe Daniel Martin, aujourd'hui conférencier, anciennement commissaire divisionnaire de la DST (direction de la surveillance du territoire) et fonctionnaire international à l'OCDE (organisation de coopération et de développement économique) devenu spécialiste des nouvelles technologies. Et des arnaques liées à internet. Le président de l'Institut International des Hautes Études de la cybercriminalité était présent à Limoges ces jours-ci, à l'invitation de la CCI de Limoges et du club des décideurs du Limousin.

1. Les cibles. Pour Daniel Martin, l'explosion des réseaux entraîne une forte hausse des arnaques, délits et autres surveillances illégales. Ces menaces pèsent sur trois catégories :

Les particuliers : « Trois milliards de personnes dans le monde sont connectés sur les réseaux. Soit autant de paires d'yeux qui peuvent rentrer par la fenêtre de l'ordinateur que vous venez d'ouvrir ». Entre 0,1 et 0,3 % des gens auraient, selon lui, des activités criminelles liées à la finance. « Sur trois milliards de personnes, ça fait beaucoup », résume-t-il. Pour lui, l'un des risques majeurs reste l'usurpation d'identité. « On utilise votre nom, vos coordonnées bancaires. 120.000 personnes se font chaque année en France usurper leur identité. »

Les entreprises : Les pillages de fichiers clients, le vol des secrets d'entreprises sont quelques-unes des menaces qui pèsent sur les sociétés.

En matière d'appel d'offres, des entreprises ont déjà pénétré le réseau informatique des concurrents pour connaître le montant qu'il proposait dans le cadre d'un marché.

Les États et les services : « À partir du moment où tout est branché en réseau, même un réseau interne, on peut le modifier. On peut modifier, par exemple, les appareils dans les hôpitaux qui distribuent de l'insuline et tuer quelqu'un à distance, faire exploser un groupe électrogène ou dérégler des centrales d'eau potable. Ce sont des menaces réelles. Les terroristes emploient des ingénieurs très compétents. En Pologne, un pirate informatique a modifié le système électronique d'un tramway, provoquant la mort d'une personne. C'est simple, les Américains disent craindre aujourd'hui un Pearl Harbor informatique ».

2. Les moyens utilisés. Les pirates informatiques utilisent toutes sortes de techniques que détaille Daniel Martin : le « phishing », par exemple, qui consiste à lancer un hameçon virtuel sur le net pour voler l'identité, l'adresse, les codes bancaires de la victime. « Vous recevez un message d'EDF vous disant de donner vos références bancaires, sinon on vous coupe l'électricité. Parfois, c'est la caisse d'allocations familiales qui vous annonce qu'elle vous doit de l'argent… Derrière se trouvent des pirates. »

6.4.1.1.2 commerce

6.4.1.1.2.1 carte bancaire

Fraude à la carte bancaire. Quelques chiffres : http://www.fia-net-group.com/wp-content/uploads/2013/04/CP_Certissim_Livre_Blanc_2013_La-fraude_sur_Internet_120413.pdf

Communiqué de Presse Paris, le 12 Avril 2013

FIA-NET publie son Livre Blanc Certissim 2013 sur la fraude à la carte bancaire sur Internet

Au cours de l'année 2012, avec 26 millions de transactions analysées pour un chiffre d'affaires de plus de 4 milliards d'euros, Certissim a constaté un taux de tentatives de fraude de 2,98 % en nombre et de 3,91 % en valeur. Cependant, moins d'une tentative sur trente se traduit par un impayé frauduleux pour les e-commerçants.
En supposant que tous les sites marchands disposent d'un système de lutte contre la fraude efficace et en extrapolant ces analyses à l'ensemble du e-commerce français, soit 45 milliards d'euros de chiffre d'affaires[1], les tentatives de fraude auraient représenté plus de 1,7 milliard d'euros en 2012.

6.4.1.1.3 Etats

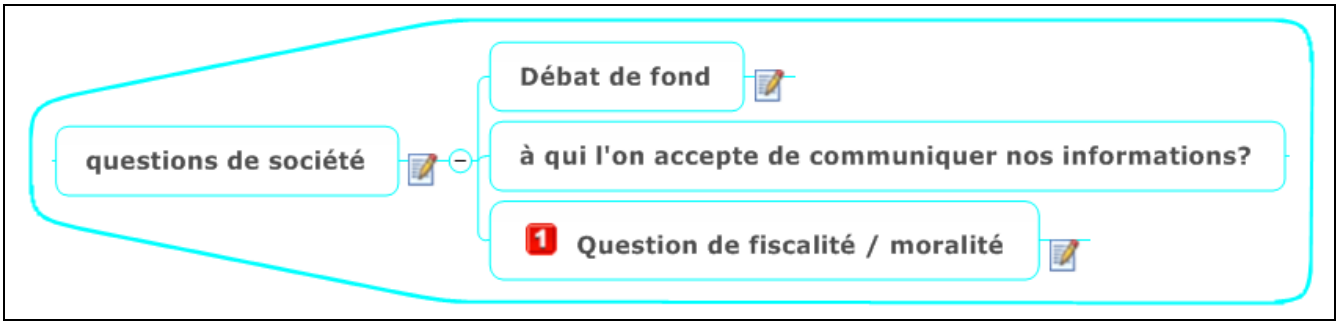
6.4.1.1.3.1 profil de la personnalité

CEDIDAC. CENTRE DU DROIT DE L'ENTREPRISE DE L'UNIVERSITÉ DE LAUSANNE : http://www.unil.ch/webdav/site/cedidac/shared/Bulletins/Bulletin_no_57.pdf

2) La collecte des informations de géolocalisation en Europe et en France

Avec l'exemple d'*Apple*, il est certain que la société connaît aussi bien le numéro de série de l'appareil (identifiant unique), son identification *IMEI* ou *ICCID*[46], ainsi que les données personnelles telles que le nom, l'adresse, le numéro de téléphone, le sexe, les informations de la carte de crédit, sans compter les réponses aux questions secrètes *etc*. grâce notamment à leur service centralisé de synchronisation et de gestion de la musique et des applications *iTunes*. *Apple* n'a donc pas besoin qu'un opérateur télécom lui fournisse ces informations puisqu'elle les obtient par un autre moyen. De plus, en tant que concepteur et développeur du système d'exploitation du téléphone (*iOS*), *Apple* pourrait même y avoir programmé un identifiant unique supplémentaire, encore tenu secret. Ces données, couplées aux relevés de localisation, permettent, selon nous, d'établir des profils de la personnalité relativement bien détaillés – fréquentation de lieux publics tels que restaurants, hôpitaux, centres de loisirs, centres religieux, centres commerciaux, emplacements des domiciles privé ou professionnel, lieux de vacances ou de voyages, habitudes diverses, *etc*.[47]

6.5 questions de société



6.5.1 Etat : Débat de fond

Voir le(s) document(s): confidence-in-the-judicial-system-is-important-for-confidence-in-national-government_gov_glance-2013-graph7-en;jsessionid=1ug58v8ci8fpm.x-oecd-live-01

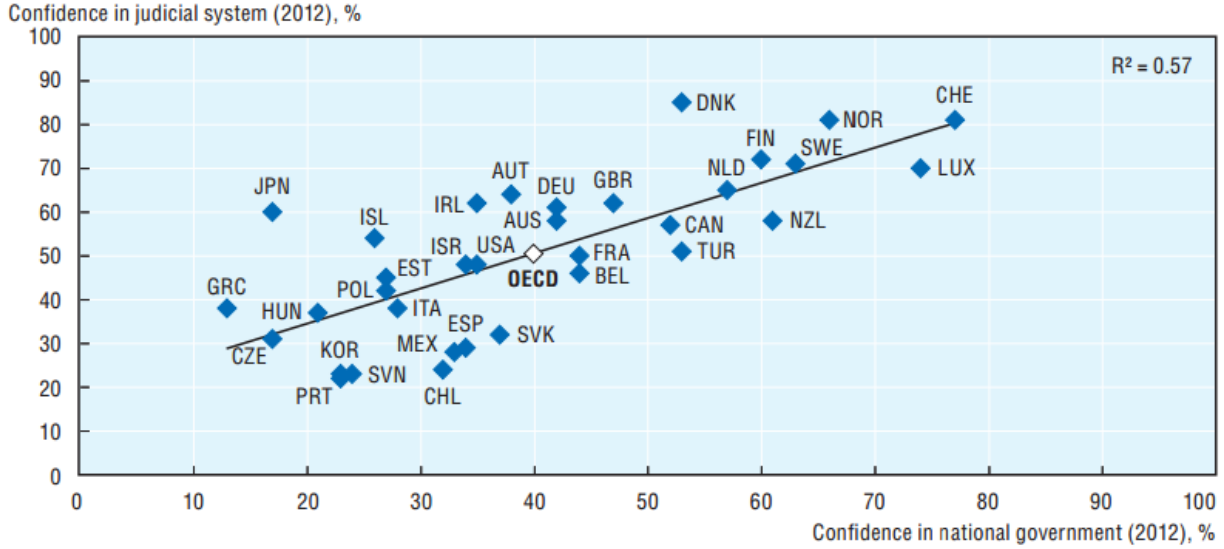
Lutte anti-terroriste, souveraineté, sauvegarde de la sphère privée et protection des intérêts économiques compatibles?

Government at a Glance - 2013

http://www.oecd-ilibrary.org/governance/government-at-a-glance-2013/confidence-in-the-judicial-system-is-important-for-confidence-in-national-government_gov_glance-2013-graph7-en;jsessionid=1ug58v8ci8fpm.x-oecd-live-01

Figure 1.6. **Confidence in the judicial system is important for confidence in national government**

Correlation between confidence in national government and confidence in the judicial system (2012)



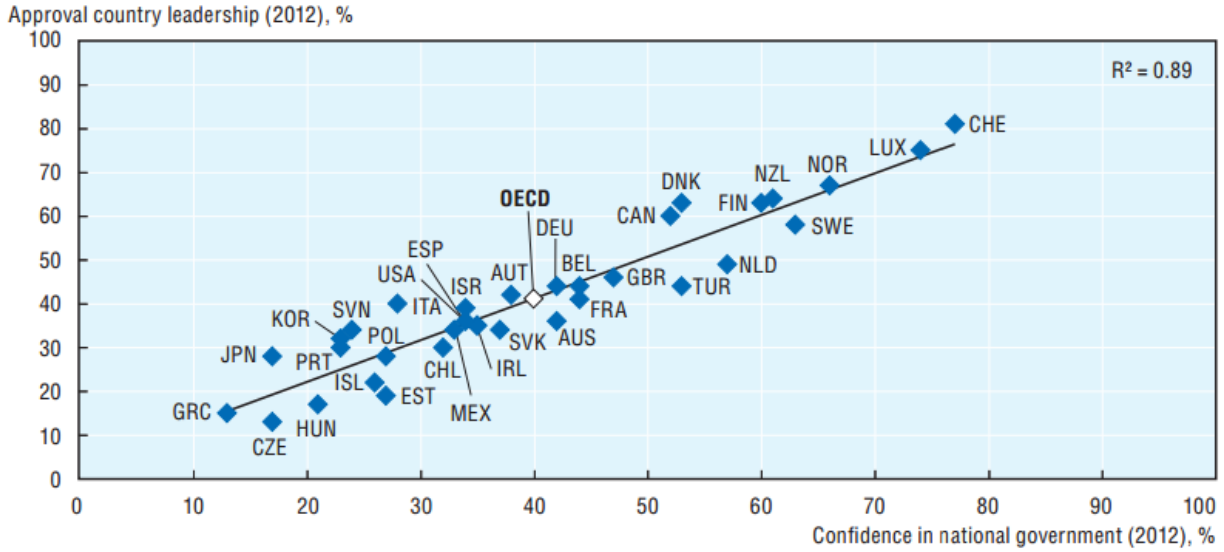
Note: Confidence in national government data refer to percentage of "yes" answers to the question: "In this country, do you have confidence in each of the following, or not? How about national government?" Confidence in the judicial system data refer to percentage of "yes" answers to the question: "In this country, do you have confidence in each of the following, or not? How about judicial system and courts?" Data for Chile, Germany and the United Kingdom are for 2011 rather than 2012.

Source: World Gallup Poll.

StatLink http://dx.doi.org/10.1787/888932940835

Figure 1.7. **Leadership is the key to confidence in national government**

Correlation between confidence in national government and leadership of the country (2012)



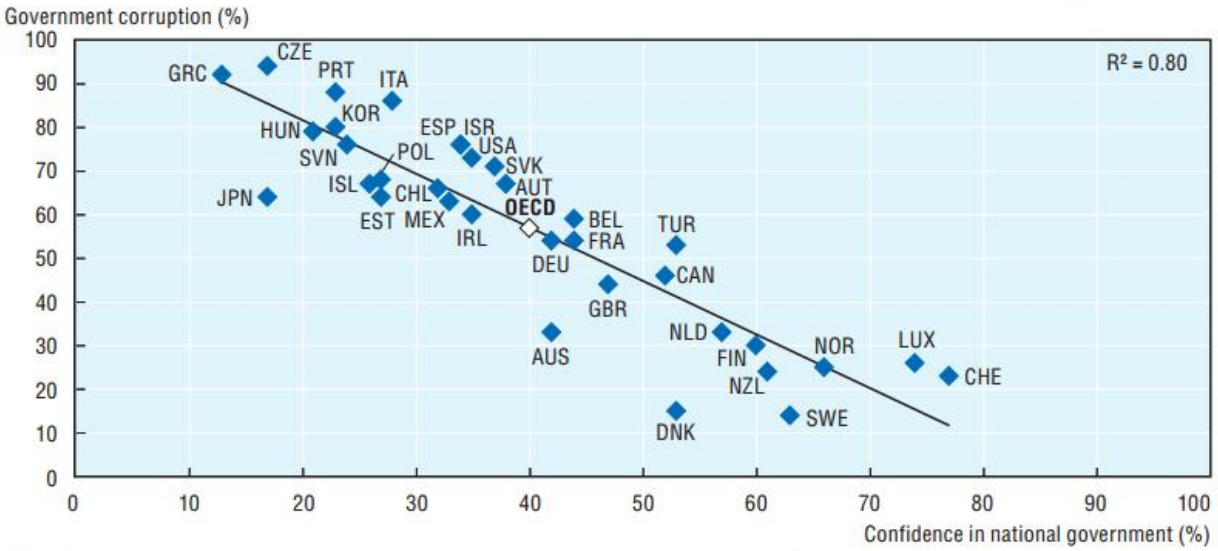
Note: Data for confidence in national government refer to the percentage of "yes" answers to the question: "In this country, do you have confidence in each of the following, or not? How about national government?" Data for approval of country leadership represent % of "approve" answers to the question: "Do you approve or disapprove of the job performance of the leadership of this country?" Data for Chile, Germany and the United Kingdom are 2011 instead of 2012.

Source: Gallup World Poll.

StatLink http://dx.doi.org/10.1787/888932940854

Figure 1.10. **Be aware of corruption!**

Correlation between confidence in national government and perception of government corruption (2012)



Note: Data for confidence in national government refer to the percentage of "yes" answers to the question: "In this country, do you have confidence in each of the following, or not? How about national government?" Data for perception of government corruption represent % of "yes" answers to the question: "Is corruption widespread throughout the government, or not?" Data for Chile, Germany and the United Kingdom are for 2011 instead of 2012.
Source: Gallup World Poll.

StatLink http://dx.doi.org/10.1787/888932940911

6.5.2 Protection de données : à qui l'on accepte de communiquer nos informations?

Voir le(s) document(s): internet-cloisonne-et-sous-monopoles-comment-a-t-on-pu-laisser-faire.html, cinq-societes-us-controlent-lacces-a-linfo.html

http://meta-media.fr/2014/03/09/internet-cloisonne-et-sous-monopoles-comment-a-t-on-pu-laisser-faire.html

Internet cloisonné et sous monopoles : comment a-t-on pu laisser faire ?

Publié le 9 mars 2014 / 3 commentaires

J'aime 227 Tweeter 269 Partager 41

Protection de données :
à qui l'on accepte de communiquer nos informations?

http://meta-media.fr/2012/08/10/cinq-societes-us-controlent-lacces-a-linfo.html

Cinq sociétés US contrôlent l'accès à l'info

Publié le 10 août 2012 / 0 commentaire J'aime 1 Tweeter 0 Partager 1

Les technologies sociales et mobiles sont en train de remodeler le paysage de l'information et poussent les médias à parier soit sur la découverte sociale de l'info, soit sur le contexte et l'immersion. Rares sont ceux qui font bien les deux, car les compétences sont différentes.

Mais dans les deux cas, résume bien Steve Rubel, associé chez Edelman et un des meilleurs experts des nouveaux médias, **cinq sociétés technologiques américaines influent ensemble sur toute l'offre d'information en ligne: Twitter, Facebook, Apple, Google et Amazon.**

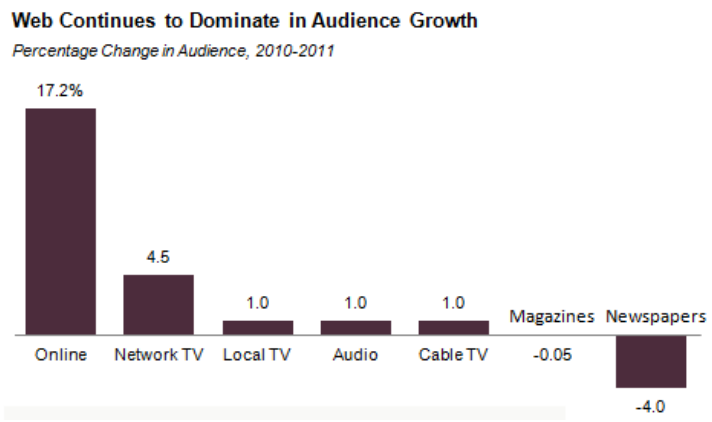
> ***"Et tous les médias sont désormais forcés de suivre tous les mouvements de ces géants, même si certains répugnent à le reconnaître (...) A court terme, les médias qui réussiront, seront ceux qui sauront comprendre, s'adapter, ou s'allier avec ces cinq entreprises".***

http://meta-media.fr/2012/03/19/medias-us-desormais-sous-domination-des-geants-de-linternet.html

Médias US désormais sous domination des géants de l'Internet

Publié le 19 mars 2012 / 0 commentaire J'aime 0 Tweeter 2 Partager 0

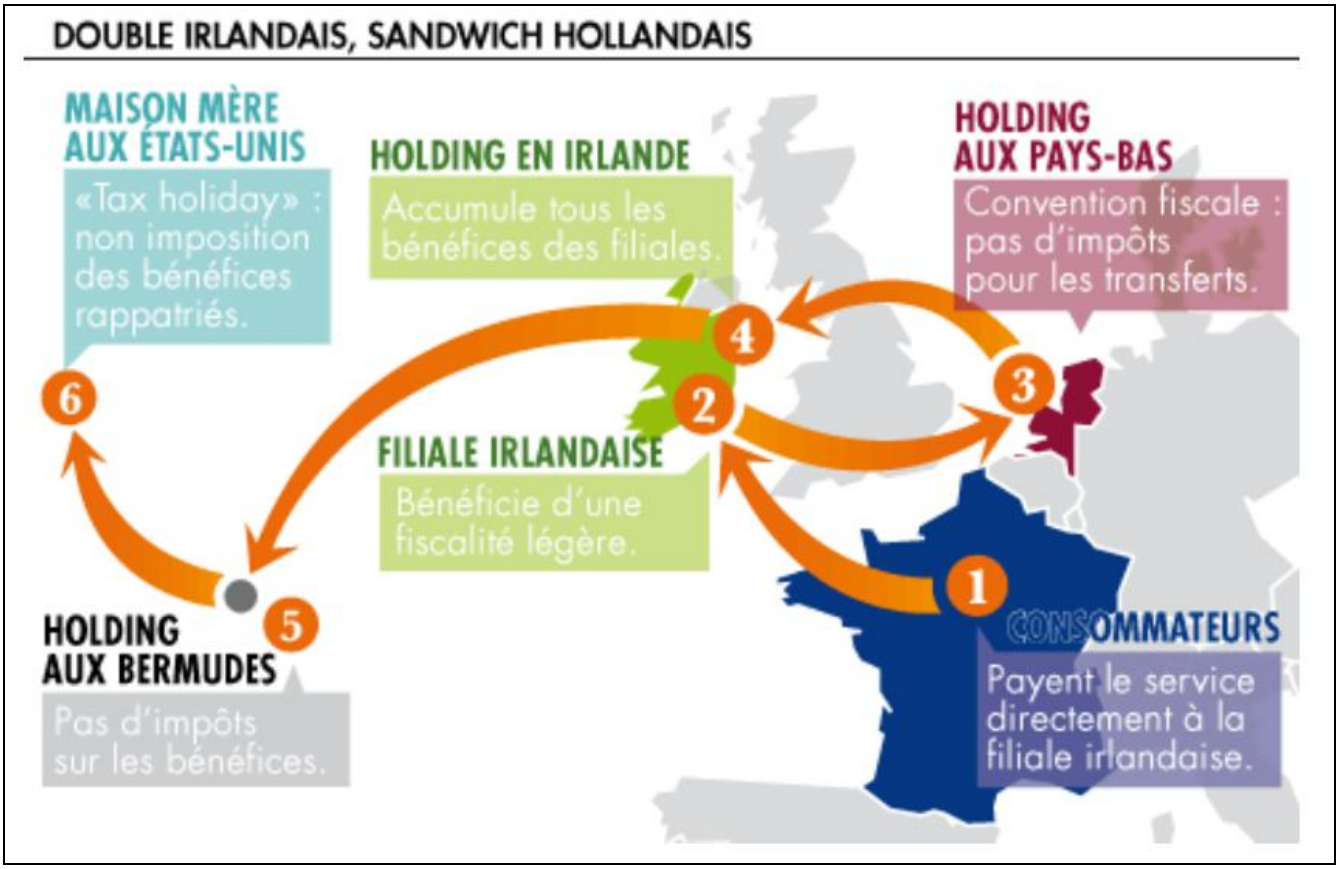
« Le secteur de l'information (américaine) n'a pas fait l'an dernier de progrès vers un nouveau modèle d'affaires et a encore perdu du terrain vis-à-vis du secteur technologique, mais l'information est devenue une part encore plus importante de la vie des gens, ce qui peut s'avérer salvateur pour le journalisme », résume ce matin la 9ème édition annuelle de l'Etat des médias américains du Pew Research Center's Project for Excellence in Journalism pour 2011.



6.5.3 Économie : Question de fiscalité / moralité

Voir le(s) document(s): 543-le-sandwich-hollandais-de-google

Économie : Question de fiscalité / moralité



http://xerbias.free.fr/blog/index.php/2011/01/04/543-le-sandwich-hollandais-de-google

Le sandwich hollandais de Google

Par xerbias, mardi 4 janvier 2011 à 19:24 :: Economie :: #543 :: rss

Le sénateur Philippe Marini a fait voter une loi taxant l'achat de publicités en ligne, une façon pour lui de trouver un moyen de ponctionner les sites web qui opèrent en France mais sont basés à l'étranger, et échappent ainsi à l'impôt français. Cet impôt supplémentaire fut rapidement affublé du sobriquet "taxe Google", en référence au leader de la recherche sur internet et de la publicité en ligne (entre autres), dont le centre de profit est en effet basé en Irlande. Avec un taux d'impôt sur les sociétés de 12,5 %, l'Irlande est en effet un pays bien plus attractif pour les entreprises étrangères souhaitant s'implanter en Europe que la France, où ce taux est de 33 %. La loi en question semble bien difficile à appliquer, et suscite les protestations du monde de l'internet. Mais si ça peut consoler Philippe Marini, le dumping fiscal de l'Irlande ne lui rapporte pas beaucoup en taxes sur ce coup là. C'est ce qu'a découvert l'agence Bloomberg en octobre dernier, en révélant que par un montage financier, Google ne payait que 2,4 % d'impôts sur la quasi-totalité des bénéfices réalisés en dehors des Etats-Unis. Le mécanisme en question arbore la pittoresque appellation de "sandwich hollandais".

Bien que complexe, Bloomberg l'explique assez bien sur le site de Business Week. La maison mère américaine créé une société irlandaise, Google Ireland Holdings, puis celle-ci en crée une autre, Google Ireland Ltd. Cette dernière est le centre d'activité, qui engrange le chiffre d'affaires en commercialisant les mots clés, et réalise donc les profits. Sauf que pour éviter l'imposition irlandaise, bien que réduite, *Holdings* fait payer un coût énorme à *Ltd* pour le droit d'utiliser la technologie Google, un artifice qui fait passer les bénéfices pour des frais, et donc non taxable. L'artifice en question est encore plus détaxé en faisant passer ce flux d'argent via une troisième société, basée cette fois-ci aux Pays-Bas, Google Netherland Holdings BV, qui n'a aucun employé. La clé de l'affaire, celle qui permet à Google Ireland Holdings de ne pas payer d'impôt, est d'affirmer que celle-ci a en fait son management (en l'occurrence, trois hommes de pailles d'un cabinet de juristes) basé à l'étranger... comme par hasard dans un paradis fiscal, les Bermudes.

Aux Etats-Unis, les comptes sont consolidés en ne prenant en compte que les impôts effectivement payés. Dans le sandwich hollandais, les deux tranches de pain sont les deux sociétés irlandaises, et se trouve au milieu la société fantôme hollandaise. Ce mécanisme aurait permis à Google de ne pas payer 3,1 milliards de dollars d'impôts sur les trois dernières années. Et bien sûr, de nombreuses autres entreprises américaines de haute technologie emploieraient un procédé analogue.

Ce n'est pas de la fraude, c'est légal. De tels grands groupes ont les moyens de faire appel à des bataillons d'avocats fiscalistes qui trouveront bien des vides juridiques pour ne pas payer des sommes importantes. C'est légal, mais c'est tout à fait immoral. L'impôt sur les sociétés est une façon pour chaque entreprise de contribuer à la société en payant sa part. Les simples particuliers, eux, pourront à raison s'estimer lésé en voyant qu'ils sont en fin de compte les seuls à payer. Lorsqu'on parle de moralisation du capitalisme, on est en plein dans le sujet avec cet exemple. Ceux qui prennent ce genre de décisions contourne l'esprit de la loi, le savent, et s'en félicitent. Comment s'étonner après des réactions hostiles que ce type de comportements engendrent ?

http://www.lafinancepourtous.com/Decryptages/Articles/Des-circuits-d-optimisation-fiscale-qui-passent-par-l-Europe

Le double irlandais avec sandwich hollandais : l'exemple d'Apple

Apple a fait l'objet d'une enquête détaillée sur ses circuits d'optimisation fiscale par le *New York Times* publiée le 28 avril 2012. Selon le journal américain, Apple fait figure de leader et de pionnier. Elle a été la première à mettre en œuvre la technique comptable connue sous le nom de "Double irlandais avec sandwich hollandais," qui réduit des impôts en acheminant les profits vers les Caraïbes via des filiales irlandaises et des Pays-Bas.

En 2012, la compagnie internationale Apple Inc. déclare un chiffre d'affaires de 156,5 milliards d'euros, elle est taxée sur ses bénéfices à hauteur de 25,2 %. Mais 61 % de son chiffre d'affaires est réalisé à l'international soit 95,5 milliards d'euros. Sur ses activités à l'étranger, Apple n'est taxé sur ses bénéfices qu'à 1,9 % ! Comment cela est-il possible ?

ANNÉE	CHIFFRE D'AFFAIRES	BÉNÉFICES AVANT IMPÔT	IMPÔTS SUR BÉNÉFICES	TAUX D'IMPÔT SUR BÉNÉFICES
2012	156,5 Mds €	55,8 Mds €	14,0 Mds €	25,2 %
dont international	95,5 Mds €	36,8 Mds €	713 M €	1,9 %
2011	108,2 Mds €	34,2 Mds €	8,2 Mds €	24,2 %
dont international	66,4 Mds €	24,0 Mds €	602 M €	2,5 %
2010	65,2 Mds €	18,5 Mds €	4,5 Mds €	24,4 %
dont international	36,6 Mds €	13,0 Mds €	161 M €	1,2 %
2009	42,9 Mds €	12,0 Mds €	3,8 Mds €	31,8 %
dont international	20,6 Mds €	6,6 Mds €	310 M €	4,7 %

Source : Comptes d'Apple Inc. (exercice clos fin septembre)

- Quand Apple vend un produit sur le sol américain, les montants collectés sont reversés à une filiale irlandaise au titre de royalties sur des brevets que cette société possède.
- Quand Apple vend à l'étranger, les produits de cette vente sont versés à une autre filiale située sur le sol irlandais : **double irlandais**
- L'Irlande a signé des traités fiscaux qui exonèrent d'impôt certains transferts intra-européens. Apple est donc obligée de faire transiter ces montants par une troisième filiale située cette fois dans les Pays-Bas : **sandwich hollandais**

La première filiale collecte alors les bénéfices qui sont ensuite expédiés aux Caraïbes, région dans laquelle ils ne seront pas du tout taxés. Si Apple rapatrie ces bénéfices aux États-Unis, ils seront taxés à hauteur de 35 %. La compagnie préfère donc les stocker dans les paradis fiscaux ou les réinvestir dans d'autres pays du monde, loin des regards des autorités fiscales américaines … sauf si est négocié un « tax holiday », c'est-à-dire une baisse exceptionnelle de l'imposition sur les transferts en provenance de l'étranger comme ce fût le cas sous George W. Bush en 2005. Les transferts ont alors été imposés à seulement 5 %.

Publié le : 19/07/13
Pages : 48

Plan d'action concernant l'érosion de la base d'imposition et le transfert de bénéfices

La fiscalité est au cœur de la souveraineté des pays, mais au cours des dernières années, les entreprises multinationales ont pu éviter l'imposition dans leur pays d'origine en réalisant des activités à l'étranger vers des juridictions à charge fiscale faible ou nulle pour l'entreprise. Le G20 a demandé à l'OCDE de remédier à ce problème croissant en développant un plan d'action pour lutter contre l'érosion de la base d'imposition et le transfert de bénéfices. Ce plan identifie une série de mesures nationales et internationales afin de résoudre le problème BEPS et fixe des échéances pour sa mise en œuvre.

- Accéder à la version en ligne
- Acheter la publication
- Lire le communiqué de presse

Le rapport est également disponible en anglais, allemand (version préliminaire), espagnol, portugais **(nouveau)** et bientôt en d'autres langues.

Publié le : 12/02/13
Pages : 96

Lutter contre l'érosion de la base d'imposition et le transfert de bénéfices

Le présent rapport s'ouvre sur une description des études et des données publiquement accessibles concernant l'existence et l'ampleur de ce phénomène. Il donne ensuite un aperçu des évolutions internationales qui ont un impact sur l'imposition des sociétés, et identifie les principes fondamentaux sur lesquels repose l'imposition des activités transnationales, ainsi que les possibilités d'érosion de la base d'imposition et de transfert de bénéfices auxquelles ils peuvent éventuellement donner lieu.

Le rapport conclut que les règles actuelles permettent d'accroître la part des bénéfices associés à des montages juridiques et à des droits et obligations incorporels, et de transférer légalement les risques au sein des groupes, avec pour conséquence de réduire la part des bénéfices associés aux opérations substantielles. Le rapport recommande de développer un plan d'action pour s'attaquer de manière détaillée au problème de l'érosion de la base d'imposition et du transfert de bénéfices.

- Rechercher la version électronique gratuite
- Accès pour les abonnés à la Librairie en ligne
- Lire le communiqué de presse

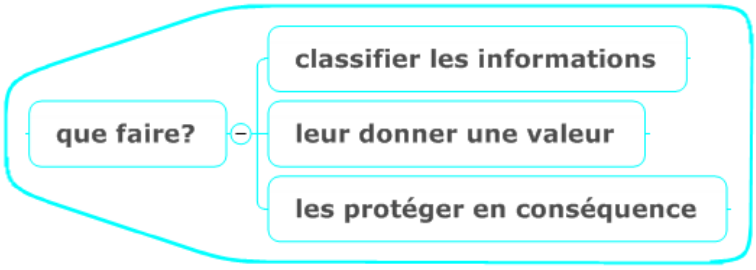
OCDE. Plan d'action concernant l'érosion de la base d'imposition et le transfert de bénéfices : http://www.oecd.org/fr/ctp/beps-rapports.htm

http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/094000486/0000.pdf

CONSEIL DES PRÉLÈVEMENTS OBLIGATOIRES

LES PRÉLÈVEMENTS OBLIGATOIRES DES ENTREPRISES DANS UNE ÉCONOMIE GLOBALISÉE

6.6 que faire?



6.6.1 classifier les informations

6.6.2 leur donner une valeur

6.6.3 les protéger en conséquence

Voir le(s) document(s): Newsletter_41_FR.pdf, EDPS-2014-04-EU-US%20trust_FR.pdf

Contrôleur européen de la protection des données (CEPD)

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Newsletters/Newsletter_41_FR.pdf

FAITS MARQUANTS

Un ensemble unique de règles pour tous: la réforme de la protection des données en Europe peut à la fois soutenir les entreprises et protéger les citoyens

La réforme des règles européennes en matière de protection des données stimulera la reprise encore fragile de l'économie européenne, a déclaré le Contrôleur européen de la protection des données après la présentation de son rapport annuel d'activités pour 2013 à la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen. La réforme de ces règles devrait être synonyme de clarté et de cohérence partout en Europe : les mêmes règles s'appliqueront à toutes les entreprises qui exercent leur activité dans l'Union européenne et les citoyens seront rassurés pour ce qui concerne le traitement de leurs informations personnelles.

Le Parlement européen a massivement voté en faveur du train de réformes qui proposera un ensemble de règles uniformes plus simples - et plus économiques - pour les entreprises traditionnelles et en ligne. Il incombe à présent au Conseil de soutenir ce train de réformes dans son ensemble en garantissant aux citoyens le droit de contrôler l'usage qui est fait de leurs informations personnelles ainsi que le droit de recours s'ils sont injustement pris pour cible ou discriminés.

Peter Hustinx, CEPD

Rapport annuel CEPD 2013

Communiqué de presse du CEPD

Rétablir la confiance entre l'UE et les États-Unis passe nécessairement par le respect du droit européen à la protection des données

L'application stricte des lois communautaires existantes en matière de protection des données est un élément essentiel pour rétablir la confiance entre l'Union européenne et les États-Unis, a déclaré le Contrôleur européen de la protection des données 5CEPD) après la publication de son avis le 20 février 2014.

Les droits des citoyens européens à la protection de leur vie privée et de leurs données personnelles sont ancrés dans le droit de l'UE. La surveillance massive des citoyens européens par les agences de renseignement américaine et autres ne tient pas compte de ces droits. En plus de soutenir de nouvelles avancées législatives en matière de vie privée aux États-Unis, l'Europe doit insister sur l'application stricte de la législation européenne en vigueur, promouvoir des standards internationaux de respect de la vie privée et adopter rapidement la réforme en cours du cadre législatif de l'UE sur la protection des données. Un effort concerté pour rétablir la confiance est nécessaire.

Peter Hustinx, CEPD

Avis du CEPD

Communiqué de presse du CEPD

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2014/EDPS-2014-04-EU-US%20trust_FR.pdf

La **surveillance** à grande échelle des communications des citoyens est **contraire** à la législation de protection des données ainsi qu'à la Charte des droits fondamentaux de l'UE. Dans une société démocratique, les citoyens devraient être **certains** que leurs **droits à la vie privée**, à la **confidentialité** de leurs communications et à la **protection de leurs données personnelles** soient respectés. Toute exception ou restriction à ces droits fondamentaux à des fins de sécurité nationale ne devrait être autorisée que si strictement **nécessaire**, **proportionnée** et **conforme** à la **jurisprudence européenne**.