Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA DÉFENSE
ET DES ANCIENS COMBATTANTS

La cyberdéfense : un effort de la nation dans toutes ses composantes

ANAJ – 16 mars 2011

DGSIC

Direction Générale des Systèmes d'Information et de Communication

Plan

- État des lieux
- Organisation nationale
- Enjeux

Défense et sécurité nationale
Le livre blanc

La France doit garder un domaine de souveraineté, concentré sur les capacités nécessaires au maintien de l'autonomie stratégique et politique de la nation : la dissuasion nucléaire, le secteur des missiles balistiques, les sous-marins nucléaires d'attaque, ***la sécurité des systèmes d'information*** *font partie de ce premier cercle*

Relevé de conclusion – « Défense et Sécurité nationale le livre blanc », éditions Odile Jacob et La documentation Française, 2008, p.318

État des lieux

Attaques ciblées

La France, comme la plupart de ses partenaires, est victime d'attaques ciblées au moyen de messages piégés.

Collection Grands Cinéastes
Premier numéro :
Chaplin

Le livre & le DVD offerts par Le Monde

Le Monde

1,30 € ou 5,20 € avec le DVD (en France métropolitaine uniquement). Ne peut être vendu sans « Le Monde TV & Radio ». www.lemonde.fr

63e ANNÉE - Nº 19479 - FRANCE MÉTROPOLITAINE — DIMANCHE 9 - LUNDI 10 SEPTEMBRE 2007 — FONDATEUR : HUBERT B

La France, cible de hackers chinois

Piratage informatique Des traces d'attaques contre des services de l'Etat ont été décelées

Comme l'Allemagne, les Etats-Unis et la Grande-Bretagne, la France a, elle aussi, été victime des cyberattaques venues de Chine. « *Depuis quelques semaines*, a indiqué au *Monde* Francis Delon, secrétaire général de la défense nationale (SGDN), *j'ai l'indication certaine que la France n'a pas été à l'abri d'attaques ciblées* » de la part de pirates informatiques (hackers) chinois. Ses services, spécialisés dans la défense et la sécurité nationales, directement rattachés à Matignon, ont décelé, explique-t-il, « *des traces d'attaque qui ont touché des services étatiques* ». Et d'ajouter : « *On peut parler d'affaire sérieuse.* »

Le 4 septembre, le *Financial Times* révélait qu'au mois de juin les ordinateurs du secrétaire américain à la défense, Robert Gates, avaient été « visités » huit jours après que la chancelière Angela Merkel se fut plainte de faits similaires en Allemagne. Le 5, c'était au tour du quotidien britannique *The Guardian* d'annoncer qu'à Londres le Foreign Office avait également été visé par des pirates électroniques. En France, les attaques ont commencé après l'élection présidentielle de Nicolas Sarkozy et ont, selon le SGDN, les « *mêmes origines* ».

M. Delon reste cependant prudent sur la responsabilité de ces intrusions dans des systèmes informatiques sensibles, qu'il ne veut pas désigner avec plus de précisions.

ISABELLE MANDRAUD

Lire la suite page 8

Marché noir : tarif de location d'un « botnet »

Country:	Price $ per 1000 uniq loads:
US	50
UK	60
NL	25
FR	25
PL	18
IT	60
DE	25
ES	25
AU	100
GR	25
Other	18
Asia	3

Pour mémoire :

- taille estimée de l'attaque estonienne : 2000 machines
- coût moyen de... 100 $

Sabotage matériel

- Des lecteurs de cartes bancaires à piste magnétique piégés
- Des centaines de lecteurs de cartes destinés aux commerçants européens ont été modifiés par un groupe criminel chinois et pakistanais.
- Ces délinquants ont ajouté des composants afin de récolter des informations bancaires, dont les codes secrets des porteurs.

Chip and pin scam 'has netted millions from British shoppers' - Telegraph http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/31...

Telegraph.co.uk

Chip and pin scam 'has netted millions from British shoppers'

A sophisticated "chip and pin" scam run by criminal gangs in China and Pakistan is netting millions of pounds from the bank accounts of British shoppers, America's top cyber security official has revealed.

By Henry Samuel in Paris
Last Updated: 6:28PM BST 10 Oct 2008

Comments 2 (#comments) | Comment on this article (#postComment)

Dr Joel Brenner, the US National Counterintelligence Executive, warned that hundreds of chip and pin machines in stores and supermarkets across Europe have been tampered with to allow details of shoppers' credit card accounts to be relayed to overseas fraudsters.

An investigation launched by Mastercard International is understood to have discovered several of the corrupted chip and pin machines at UK Asda and Sainsbury's Photo: PA

These details are then used to make cash withdrawals or siphon off money from card holders' accounts in what is one of the largest scams of its kind.

In an exclusive interview with The Daily Telegraph, America's counterintelligence chief said: "Previously only a nation state's intelligence service would have been capable of pulling off this type of operation. It's scary."

An organised crime syndicate is suspected of having tampered with the chip and pin machines, either during the manufacturing process at a factory in China, or shortly after they came off the production line.

In what is known as a "supply chain attack", criminals managed to bypass security measures and doctor the devices before they were dispatched from the factories where they were made.

The machines were opened, tampered with and perfectly resealed, said Dr Brenner, "so that it was impossible to tell even for someone working at the factory that they had been tampered with." They were then exported to Britain, Ireland, the Netherlands, Denmark and Belgium.

An investigation launched by Mastercard International is understood to have discovered several of the corrupted machines at British branches of Asda and Sainsbury's.

In all, hundreds of devices in Britian and other affected countries had been copying the account details and pin numbers of thousands of credit and debit cards over the past nine months and transmitting the data via mobile phone networks to underworld electronic experts in Lahore, Pakistan.

Once MasterCard had uncovered the scam it alerted stores which set about examining tens of thousands of chip and

Contrôle des systèmes vitaux (1/2)

- Pologne: Un adolescent blesse douze personnes en prenant le contrôle, à l'aide d'une télécommande, des aiguillages du tramway de la ville de Lodz
  - ✓à partir d'informations recueillies au dépôt des tramways, il avait modifié une télécommande infrarouge pour contrôler des aiguillages et ensuite, par jeu, en manipuler trois, entraînant divers incidents.
- La CIA a indiqué que des individus malveillants avaient déjà, dans plusieurs régions du monde, pris le contrôle de systèmes SCADA depuis Internet afin de provoquer des coupures d'électricité.
  - ✓Les attaquants se seraient parfois livrés à des manœuvres d'extorsion, menaçant de couper l'électricité à défaut de paiement.

Contrôle des systèmes vitaux (2/2)

- 5 mai 2008: Vulnérabilité critique touchant des systèmes informatiques de contrôle industriel déployés dans plus de 100 000 usines dans le monde :
  - ✓déployé dans un tiers des usines ayant des systèmes SCADA, le logiciel Wonderware Suitelink a présenté pendant quatre mois une vulnérabilité pouvant permettre de couper à distance les systèmes industriels de supervision concernés.
- Et en 2010... Stuxnet
  - ✓Une attaque ciblant sans doute le programme nucléaire iranien
  - ✓Quatre zero-day
  - ✓Des clés racines d'éditeurs compromises
  - ✓Des « air gaps » franchis

La menace évolue

- 1998 : Tchernobyl (CIH) : déni de service local
- 2003 : Blaster : déni de service distribué sur Microsoft
- 2007 : L'Estonie est attaquée de façon coordonnée
- 2010 : Stuxnet : attaque sur des systèmes de contrôle industriels (SCADA) ciblés

- Le niveau de menace augmente

- La réponse à ce niveau de menace a besoin d'être :
  - coordonnée et organisée
  - soutenue et financée
  - généralisée

Organisation nationale

Une autorité nationale : l'ANSSI

- Le constat avait été fait dès avant le livre blanc
  - Rapports du député Lasbordes et du sénateur Romani
  - La sécurité des systèmes d'information a besoin d'une autorité centralisée et incontestable
- L'ANSSI a été créée par décret n°2009-834 du 7/7/2009
  - C'est un service à compétence nationale
    - La forme la plus autonome d'une administration régalienne
  - Elle est « l'autorité nationale en matière de SSI » (art. 3)
  - Elle opère un centre de détection sur les SIC de l'État (art. 3)
  - Elle qualifie les produits et prestataires de SSI (art. 4)
  - Elle apporte son soutien aux ministères en charge des opérateurs de communications électroniques et d'importance vitale (art. 5)
  - Elle oriente la R&D et promeut la SSI (art. 6)

Une autorité : deux missions

- Par le décret récent n°2011-170 du 11/2/2011 l'ANSSI se voit aussi confiée la mission d'assurer « la fonction d'autorité nationale de défense des systèmes d'information »
- Ces deux missions sont complémentaires :
  - La « protection des systèmes d'information et de communication » (PSIC) consiste à mettre en place des mécanismes de défense en profondeur des SIC
  - La « défense des systèmes d'information et de communication » (DSIC) consiste à exploiter ces défenses mises en place pour conduire les opérations de réaction aux attaques informatiques

Une autorité soutenue

- L'ANSSI, interministérielle, est rattachée au Secrétaire général de la défense et de la sécurité nationale
- D'autres acteurs importants sont présents dans l'organisation nationale
  - Ils apparaissent à l'article 7 du décret 2009-834 dans la composition du « comité stratégique de la SSI »
    - Ministère de la défense
      - CEMA, DGA, DGSE, DGSIC
    - Ministère de l'intérieur
      - SG, DCRI
    - Ministère des affaires étrangères
      - SG
    - Ministère de l'économie et des finances
      - DGME, CGIET

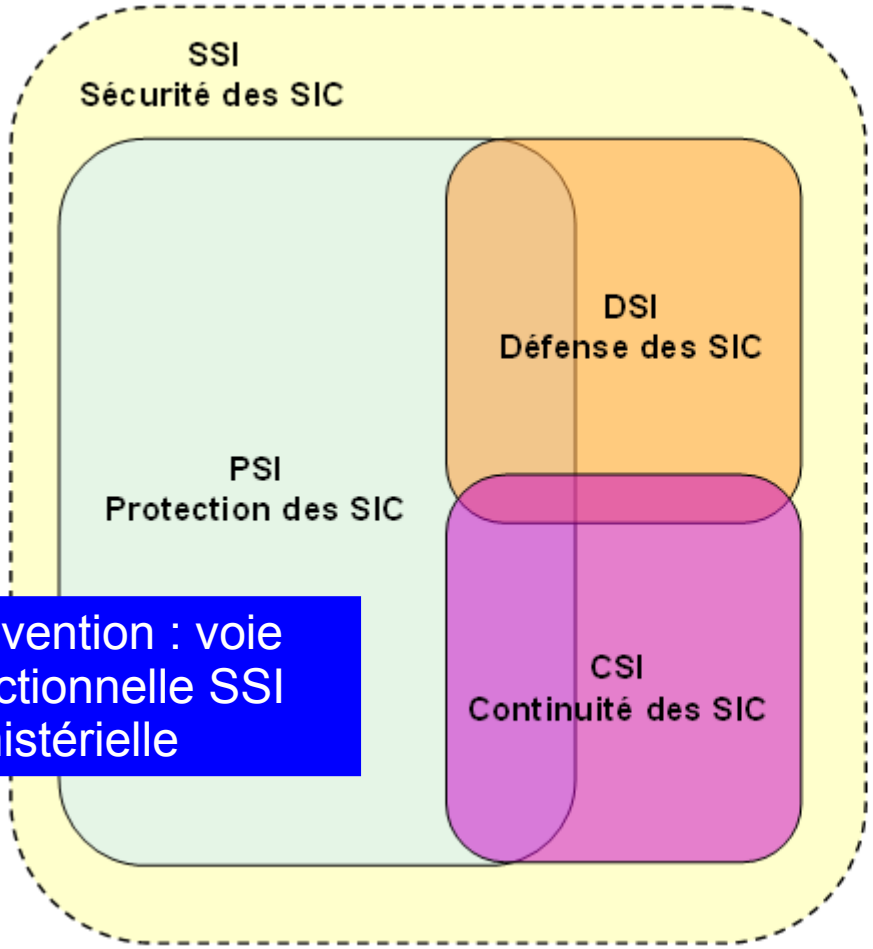
Des rôles complémentaires

- Ministère de la défense
  - Effort de R&D pour les produits de sécurité souverains
  - Soutien logistique et humain en cas de crise majeure (opérateur autonome)
  - Renseignement extérieur
- Ministère de l'intérieur
  - Lutte contre la cybercriminalité (OCLCTIC, IRCGN)
  - Relais territoriaux (OZSSI)
  - Renseignement intérieur
- Ministère des affaires étrangères
  - Coopérations internationales
- Ministère de l'économie et des finances
  - Administration électronique
  - Tutelle des opérateurs de télécommunication

Sécurité des systèmes d'information de l'État

- Chaque ministre reste responsable de la sécurité de ses systèmes d'information et de communication
  - En particulier il assure la « continuité des SIC »
- Comme pour les autres domaines de la sécurité nationale, le SGDSN coordonne les hauts fonctionnaires de défense et de sécurité (HFDS) de chaque ministère
- Ces HFDS disposent, pour les aider dans le domaine particulier de la SSI, d'un fonctionnaire de sécurité des systèmes d'information (FSSI), qui sont les correspondants naturels de l'ANSSI.
  - Le rôle des HFDS/FSSI est un rôle de préparation à la gestion des crises informatiques
  - Ils n'ont pas de rôle de conduite opérationnelle dans leur résolution

Responsabilités ministérielles



ANSSI : COSSI et centre de détection interministériel

Cyber-attaques

Sinistres accidentels

Prévention : voie fonctionnelle SSI ministérielle

Centres de crise ministériels

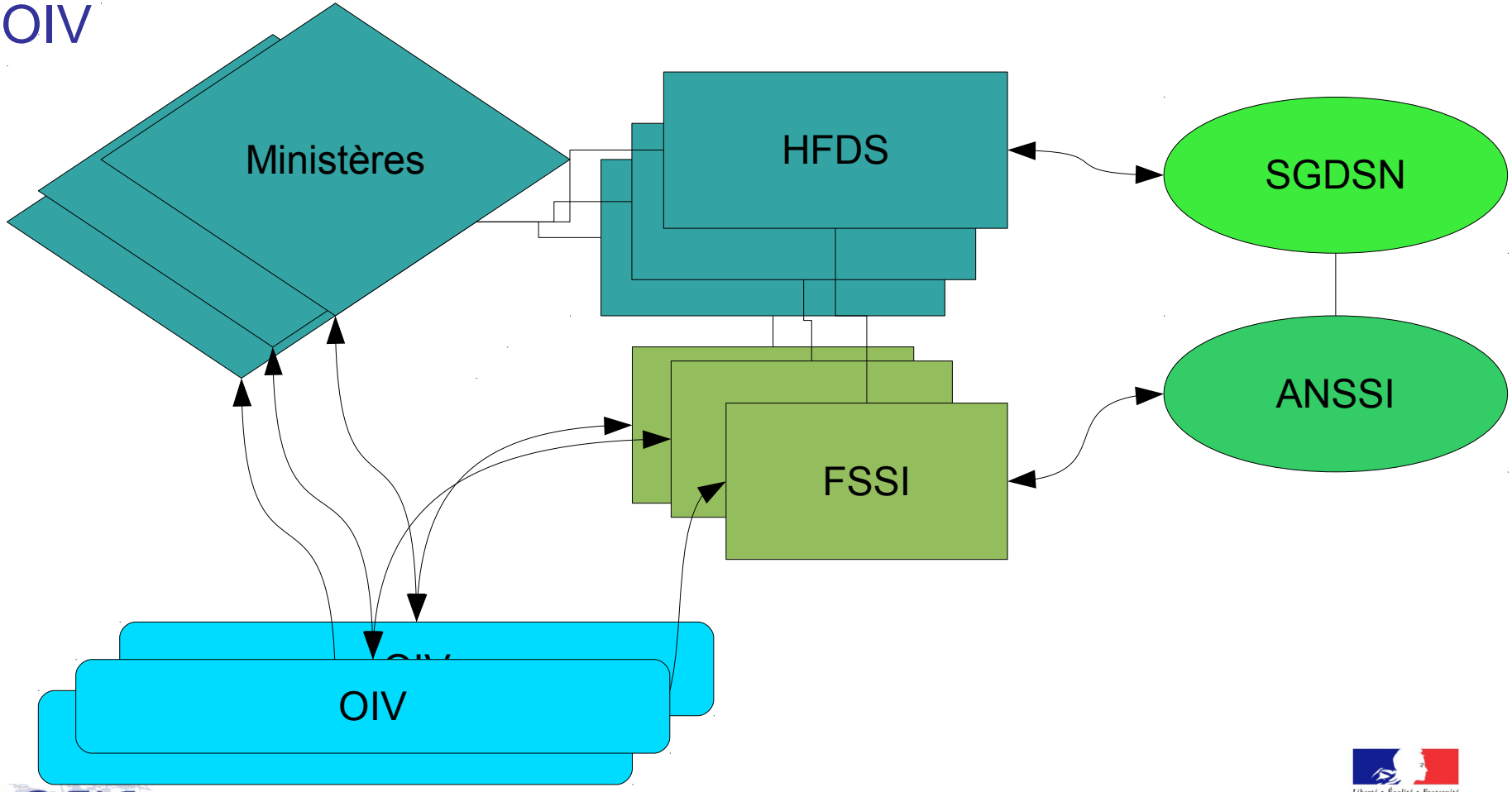
Trois réseaux

L'ANSSI anime ainsi trois réseaux de coordination

- De prévention au niveau interministériel
- De déclinaison locale
- De temps de crise

Animation interministérielle

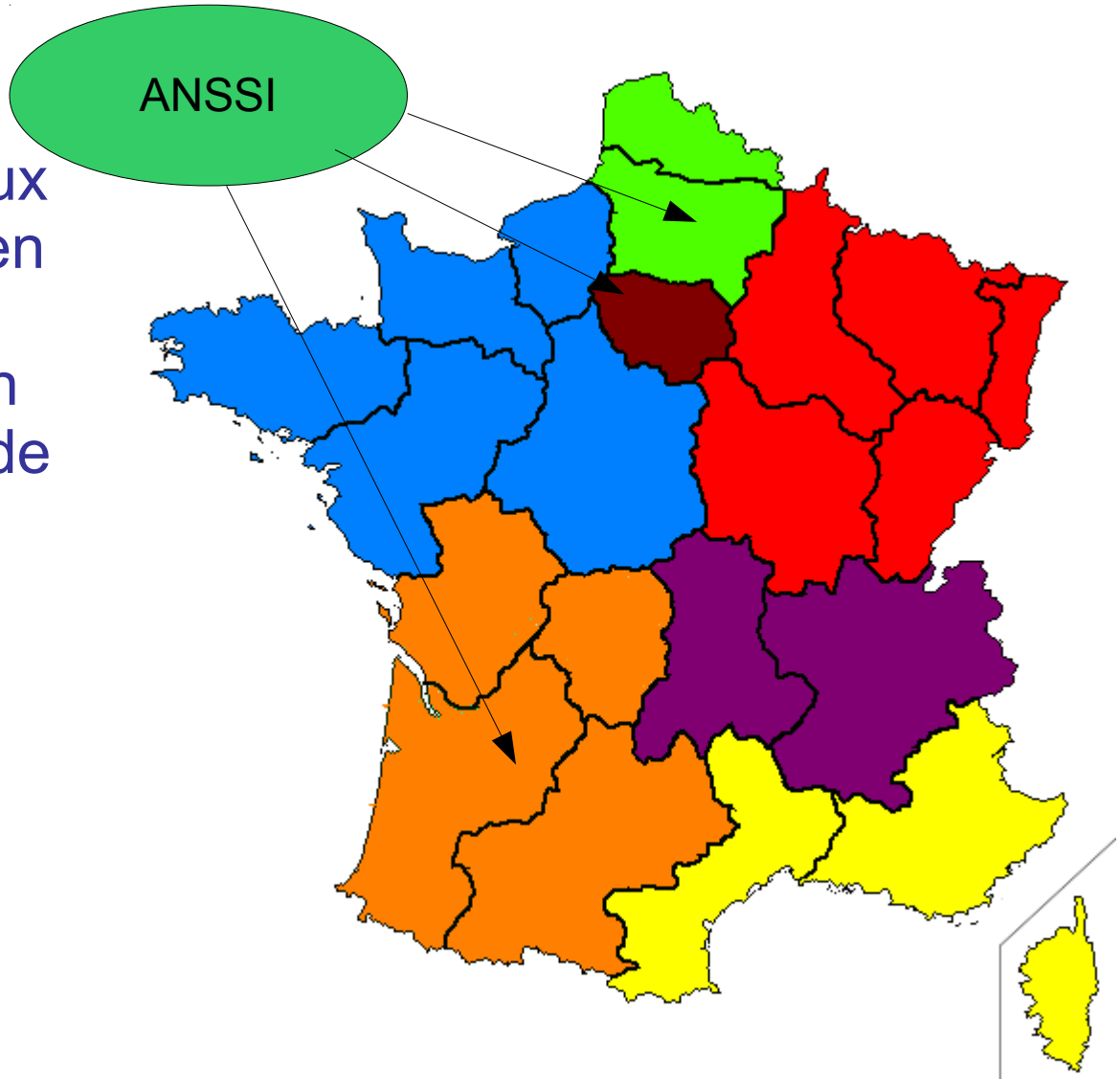
L'ANSSI coordonne la protection des SIC de l'Etat et des OIV



Animation territoriale

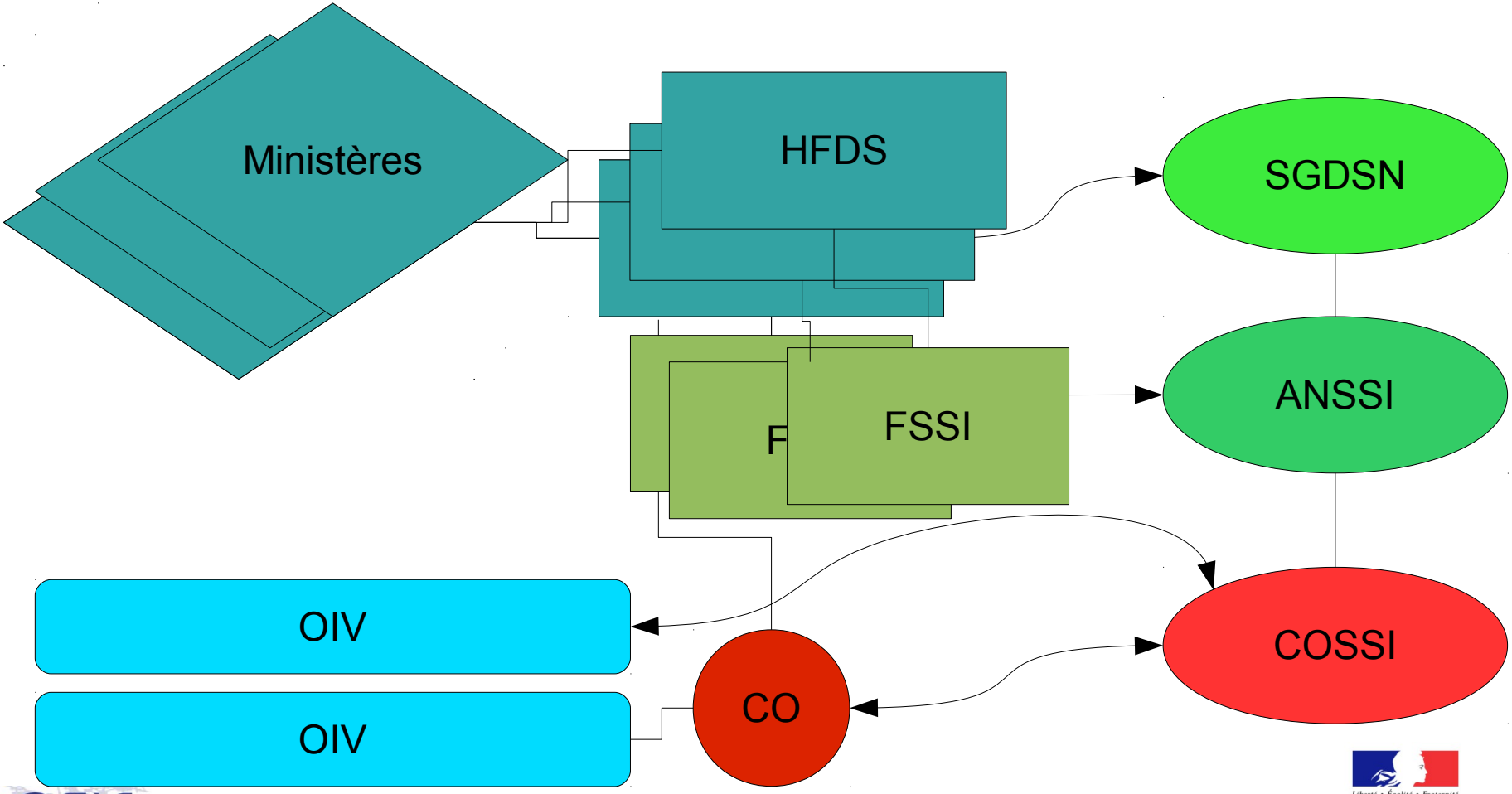
Les observatoires zonaux de la SSI mis en place en liaison avec le ministère de l'intérieur assurent un relais local aux actions de protection des SIC au service :

- Des administrations déconcentrées
- Des OIV
- Du tissu industriel



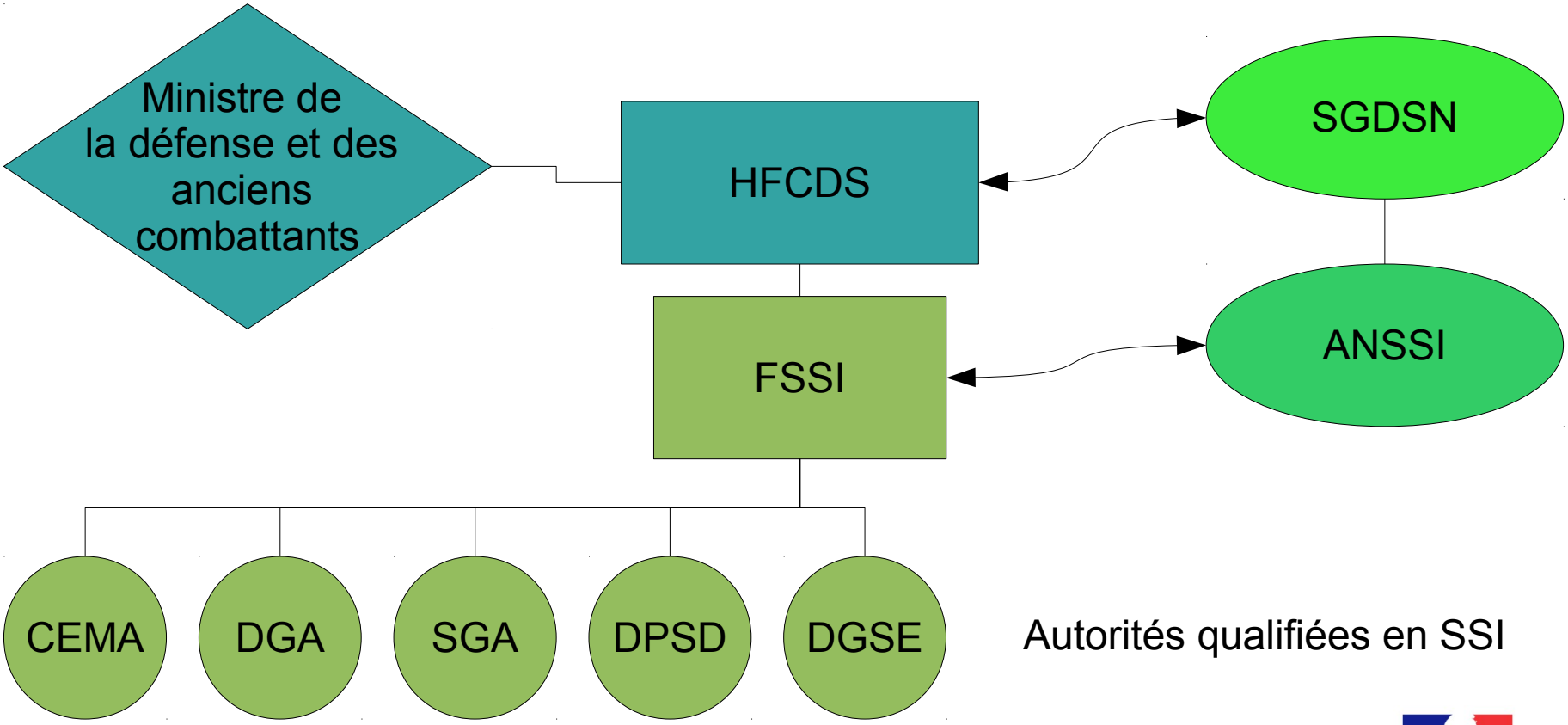
Gestion de crise

En temps de crise, le COSSI agit directement ou via les centres opérationnels des ministères



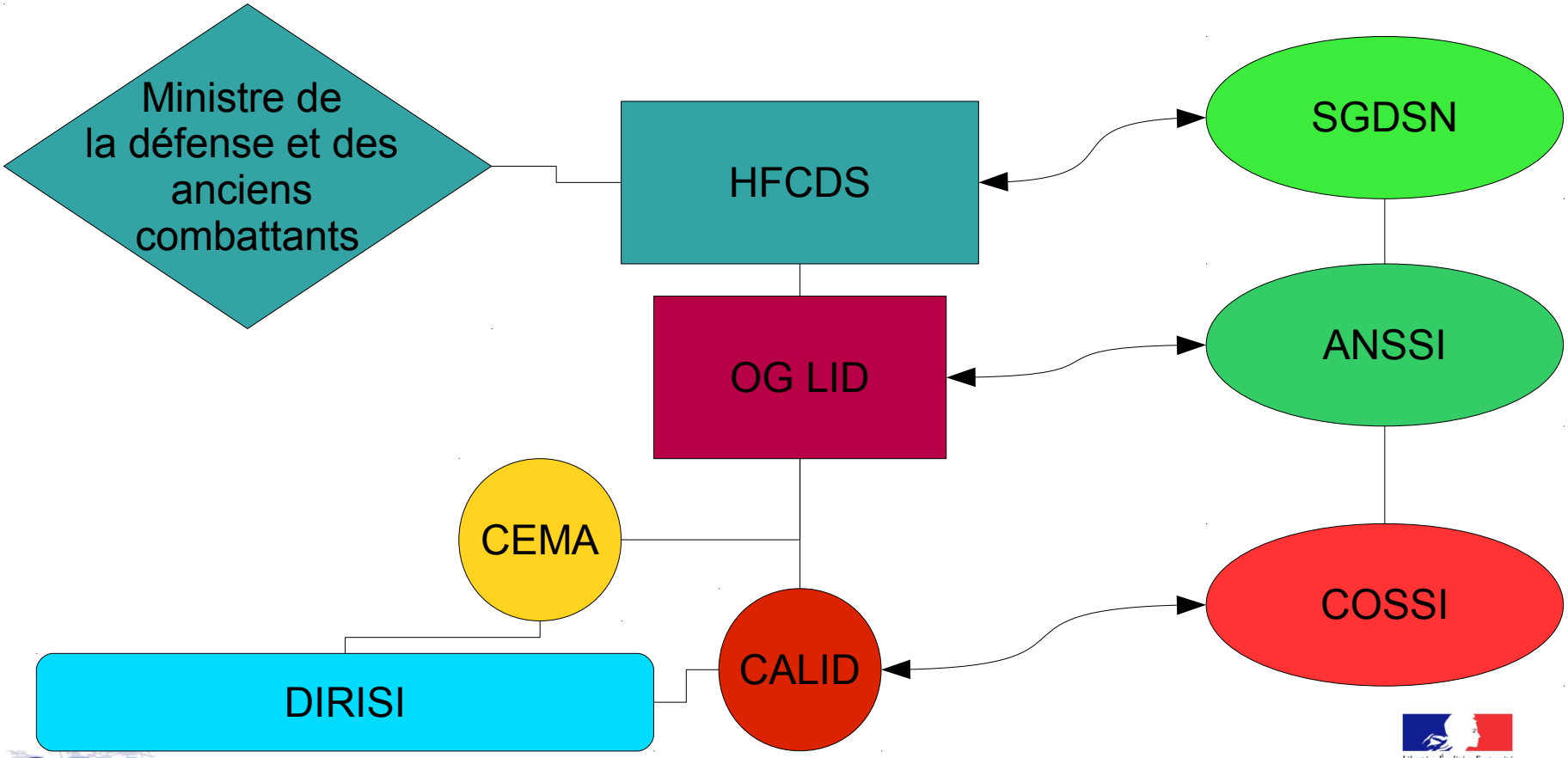
Cas du ministère de la défense

L'organisation du ministère en matière de protection des SIC n'est pas très différente des autres ministères



Particularité du ministère de la défense

En matière de défense des SIC, par contre, le MINDEF dispose de son propre centre de lutte informatique défensive et de son opérateur



Enjeux

La stratégie française en cyberdéfense

- La stratégie française en matière de cyberdéfense a été récemment publiée
  - À l'occasion de la publication du décret conférant à l'ANSSI le rôle d'autorité nationale de défense des systèmes d'information
- Quatre objectifs stratégiques
  - Être une puissance mondiale de cyberdéfense
  - Garantir la liberté de décision de la France par la protection de l'information de souveraineté
  - Renforcer la cybersécurité des infrastructures vitales nationales
  - Assurer la sécurité dans le cyberespace

Sept axes d'effort (1-2)

- Anticiper, analyser
  - Risques et menaces évoluent rapidement dans le cyberespace.
  - La défense et la sécurité de nos systèmes d'information passe par un suivi de l'actualité des technologies et par une analyse du jeu des acteurs publics ou privés.
  - Les acteurs du MINDEF dans ces domaines sont ceux
    - du renseignement : DGSE, DRM, DPSD
    - de la veille technique : CALID, DGA-MI
- Détecter, alerter, réagir
  - Le rôle de la chaîne LID

Sept axes d'effort (3)

- Accroître et pérenniser nos capacités scientifiques, techniques, industrielles et humaines
  - Il s'agit d'anticiper voire de créer les évolutions technologiques en maintenant nos capacités de recherche
  - Objectif : limiter l'avantage tactique de l'attaquant sur le défenseur
  - L'acteur principal du MINDEF dans ce domaine : la DGA

Sept axes d'effort (4)

- Protéger les systèmes d'information de l'État et des opérateurs d'infrastructures vitales
  - Il s'agit de disposer :
    - de produits de sécurité totalement maîtrisés
    - de services de confiance
    - des réseaux sécurisés résilients pour la chaîne de décision et de commandement sur le territoire métropolitain
  - Acteurs du MINDEF :
    - DGSIC comme prescripteur des architectures des SIC
    - DGA pour l'élaboration des produits et services de confiance
    - Industriels de l'armement
    - DIRISI comme opérateur des réseaux résilients du MINDEF

Sept axes d'effort (5-7)

- Adapter notre droit
  - Travaux interministériels (FSSI)
- Développer nos collaborations internationales
  - Le MINDEF développe des accords, notamment avec l'OTAN, et sous l'égide du SGDSN, dans le domaine de la cyberdéfense
- Communiquer pour informer et convaincre

Conclusion

- La France s'est résolument engagée dans une démarche de renforcement de sa posture de cyberdéfense
- L'ANSSI y joue un rôle central, voulu et assumé, car les menaces cybernétiques sont totalement transverses aux activités de la nation
- Pour autant, chaque acteur ministériel a son rôle à jouer
- Dans ce contexte, le MINDEF s'organise pour servir les axes d'effort de cette stratégie, plus particulièrement :
  - Dans l'anticipation
  - Dans la lutte informatique
  - Dans l'amélioration des moyens techniques
  - Dans la mise en place de services opérationnels résilients