Organisation de la Cybersécurité

Éric Jaeger, ANSSI/SDE/CFSSI

Journée SPECIF-Campus du 7 novembre 2014, CNAM, Paris

Quelques enjeux de la cybersécurité

Virus

DoS

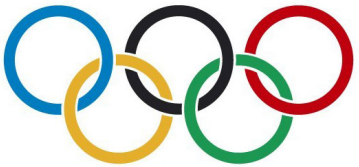
Défigurations

GAFa

Vie privée

Escroqueries

Snowden



Flame & Stuxnet

Et demain ? Domotique, internet des objets (*IoT*), *e*-sport, équipements médicaux, *e*-administration, voitures automatisées, *smart grids*, *high frequency trading*...

Une définition de la cybersécurité

Cybersécurité = SSI [1] + Cyberdéfense + Lutte contre la cybercriminalité

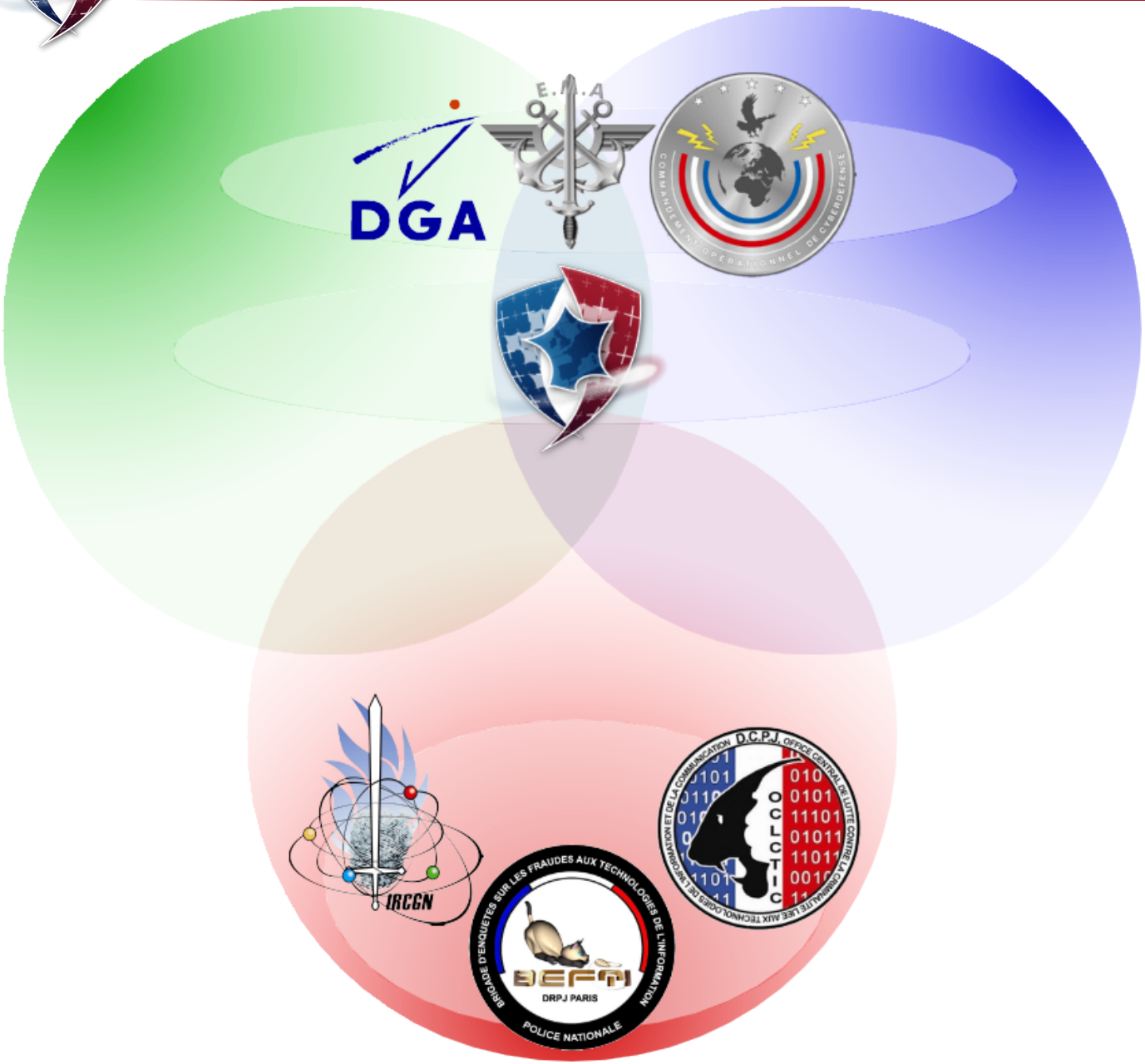
- état recherché [...] permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données [...] et des services
- fait appel à des techniques de SSI et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense (un ensemble de mesures techniques et non techniques)

Bien distinguer sûreté et sécurité (prendre en compte la malveillance)

Hors sujet : CNIL, HADOPI, D2IE, DPSD, DRM, DGSE, *etc.*

1. On parle parfois aussi de Cyberprotection

Organisation nationale de la cybersécurité



BEFTI

DGA

EMA

IRCGN

OCLCTIC

OG Cyber

Et d'autres...

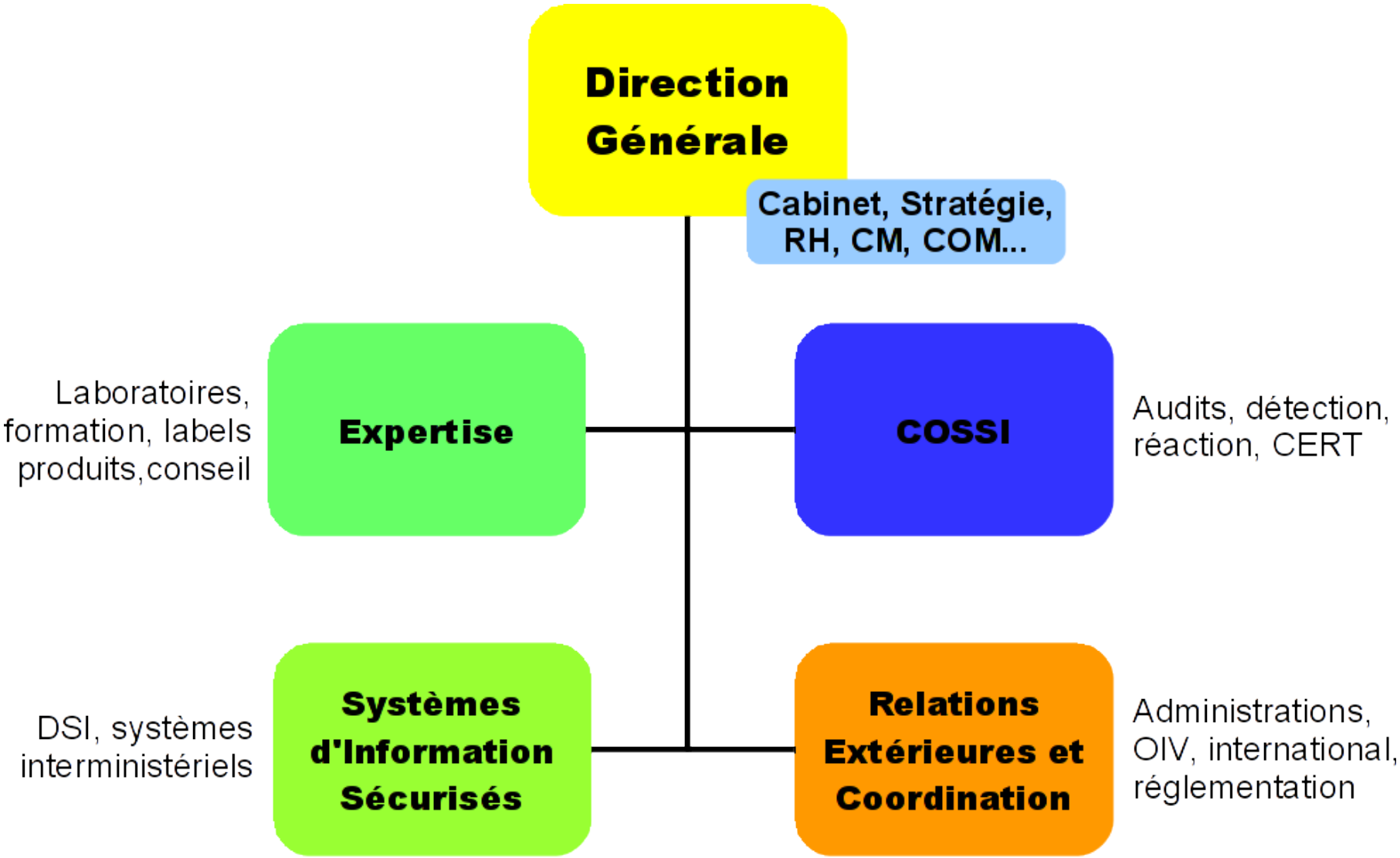
Missions de l'ANSSI

Service à compétence nationale[2] rattaché au Secrétaire général de la défense et de la sécurité nationale (Premier ministre), l'ANSSI

- décide des mesures pour répondre aux crises affectant ou menaçant la sécurité des SI des autorités publiques et des OIV
- conçoit, fait réaliser et met en œuvre les moyens interministériels sécurisés de communications électroniques nécessaires aux hautes autorités
- propose des règles pour protéger les SI de l'État et vérifie leur application
- met en œuvre un système de détection des incidents sur les SI de l'État
- qualifie des produits de sécurité et des prestataires de service de confiance
- assure la formation des personnels qualifiés dans le domaine de la SSI
- favorise la prise en compte de la sécurité dans le développement des TIC
- participe à l'orientation de la R&D de la SSI
- contribue à la promotion des des savoir-faire nationaux en SSI

2. Décret n° 2009-834 du 7 juillet 2009

Organisation de l'ANSSI



Quelques adresses

Portail de la sécurité informatique
www.securite-informatique.gouv.fr

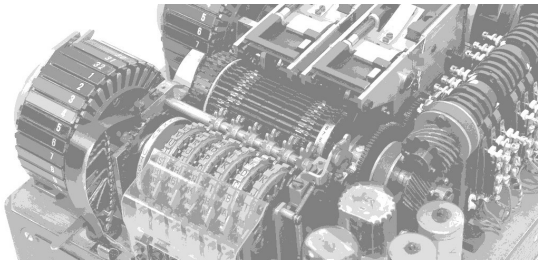
Site de l'ANSSI
www.ssi.gouv.fr

Bonnes pratiques, recommandations, guides
www.ssi.gouv.fr/fr/bonnes-pratiques/

Publications (dont articles de conférence)
www.ssi.gouv.fr/fr/anssi/publications

Formation
www.ssi.gouv.fr/cfssi

Activités du CFSSI



Au sein de la sous-direction expertise (SDE), le CFSSI développe et met en œuvre la politique formation de l'ANSSI, avec notamment

- des formations
- des relations avec les établissements de formation
- CyberEdu : l'intégration de la SSI dans les formations en informatique

Nous contacter :

- CFSSI : `cfssi@ssi.gouv.fr`
- démarche CyberEdu : `cyberedu@ssi.gouv.fr`
- adresse individuelle : `eric.jaeger@ssi.gouv.fr`

Formations au CFSSI

≪ Expert en Sécurité des Systèmes d'Information ≫

- activité historique du CFSSI (1957)
- formation longue (650 h de cours en 7 mois, puis stage 6 mois)
- certifiante (titre RNCP niveau I)
- dense et ambitieuse, strictement orientée SSI

Un catalogue d'une vingtaine de stages de formation professionnelle

- de 1 journée à plus de 4 semaines
- organisations, réglementations, techniques...
- strictement orientés SSI

Formations gratuites, réservées aux agents de la fonction publique (dont les enseignants du MENESR), les candidatures devant être validées par le service du HFDS (plus précisément le FSSI, Benoît Moreau)

Relations avec les établissements

Mises en contact, participations, promotion, identification de références

À la demande, conseil sur les programmes d'enseignement en SSI (modules, formations professionnelles ou spécialisations)

- vision parfois partielle ou biaisée de la cybersécurité
- dérive offensive fréquente, rarement pertinente, parfois illégale
- sensibiliser, éveiller à un regard différent
- enseigner SSI $\neq$ enseigner la cryptologie
- cohérence des contenus et pertinence de l'approche
- aller au-delà de la technique

Émergence de CyberEdu

Communication du conseil des ministres (mai 2011)

> *La SSI sera incluse dans les formations supérieures, en commençant par les formations scientifiques et techniques, afin que l'ensemble des étudiants acquièrent un socle commun de connaissances et de bonnes pratiques dans ce domaine.*

Feuille de route du Gouvernement sur le numérique (février 2013)

> *Un volet SSI sera intégré à toutes les formations supérieures aux métiers du numérique.*

Livre blanc sur la défense et la sécurité nationale, avril 2013

> *Il importe également d'accroître le volume d'experts formés en France et de veiller à ce que la sécurité informatique soit intégrée à toutes les formations supérieures en informatique.*

Motivations CyberEdu

La cybersécurité qui repose sur quelques spécialistes agissant de manière isolée et intervenant *a posteriori*, cela ne marche tout simplement pas

Prévenir plutôt que d'attendre de l'infrastructure qu'elle pallie !

Chaque professionnel de l'informatique devrait être sensibilisé et initié aux notions utiles et nécessaires

- ne pas introduire par ignorance des vulnérabilités
- améliorer la vigilance et la réaction aux incidents
- favoriser la coopération entre les spécialités

La sécurité devrait être abordée dès la formation initiale des informaticiens

C'est l'objectif de la démarche CyberEdu [3]

3. Initiative Anssi en coordination avec la Dgesip

Grandes orientations CyberEdu

Il ne s'agit pas de former des experts en sécurité ni même de définir de nouvelles compétences mais plutôt d'adapter les pratiques

Le nécessaire, et rien que le nécessaire, les réflexions étant à mener par métier ou compétence ; la sécurité n'est pas à traiter dans des modules dédiés mais intégrée au fil de l'eau dans les cours existants

L'approche met surtout en avant la SSI (cyberprotection), en limitant les aspects offensifs, plutôt que la cyberdéfense ou la lutte contre la cybercriminalité

La démarche CyberEdu cherche à fournir une assistance aux enseignants en informatique pour atteindre ces objectifs

Démarche CyberEdu

Différentes actions de l'Anssi lancées, prévues ou envisagées dont :

- marché d'assistance pour la rédaction de guides, l'expérimentation de la démarche, la communication
- colloques CyberEdu pour les enseignants en informatique[4]
- (TBC) animation d'une communauté, lettres, forums, *etc.*
- (TBC) labellisation des formations par l'Anssi
- ...

CyberEdu

La sécurité par l'enseignement supérieur des NTIC

4. Notamment 18-20 novembre 2014 à Paris, *cf.* `http://www.ssi.gouv.fr/cfssi`

À votre disposition pour toute question

Post scriptum : Tout ce qui précède est sans rapport avec le développement du « pôle d'excellence cyber » en Bretagne voulu par le Ministère de la défense

Le « regard » sécurité

Parmi les commandes suivantes, lesquelles sont susceptibles (sans redirection) de provoquer la destruction de données d'un fichier ?

☐ `ls` ☐ `cd` ☐ `cp` ☐ `cat` ☐ `rm` ☐ `mv`

Fonctionnel

- Question ré-interprétée « *Comment détruire les données d'un fichier ?* », seule la commande *rm* est mentionnée

Sécurité

- Si on cherche à protéger en disponibilité les données, les commandes dangereuses sont *rm* mais aussi *cp* et *mv*

Le « regard » sécurité

Un paquet *IP* comporte dans son entête deux champs adresse pour sa source et sa destination

Fonctionnel

- Rendre le service consiste à acheminer l'information jusqu'à l'adresse destination
- La diffusion convient dans certains contextes

Sécurité

- L'adresse source n'est probablement ni exploitée ni vérifiée, ce qui permet le *spoofing* d'adresse *IP*
- En diffusion, un récepteur voit l'ensemble des paquets et coopère en oubliant ceux qui ne lui sont pas adressés

Le « regard » sécurité

Spécification de deux fonctions pour la compression (Zip) et la décompression (Unzip) de fichiers

Fonctionnel

- $\forall\,(f : \text{File}),\ \text{Unzip}(\text{Zip}\,f) = f$

Sécurité

- $\forall\,(c : \text{File}),\ (\neg\exists\,(f : \text{File}),\ \text{Zip}\,f = c) \Rightarrow \text{Unzip}\,c = \text{Error}$
- En particulier, ne pas avoir confiance en un champ annonçant à l'avance la taille du fichier décompressé

Le « regard » sécurité

L'envoi de données malléables à un interpréteur peut permettre des attaques par injection, l'exemple bien connu étant entre PHP et SQL[5]

```
$cmd="SELECT * FROM Students WHERE id='".$val."'";
$dbr=mysqli_query($dbc,$cmd) or die("DB error");
```

Mais ce principe est très générique, applicable à d'autres contextes

- `Sys.command` en OCAML
- `eval` ou `$x()` en PHP
- `open` en RUBY pour les noms de fichiers commençant par `|`
- Désérialisation contrôlée (JAVA) ou pas (PYTHON)
- `printf` en C avec la balise `%n`
- `rm *` en *Shell* UNIX en présence d'un fichier nommé `-fr`
- ...

5. Ici par exemple si `$val` vaut `"Bobby'; DROP TABLE Students; //"`

Enseigner la SSI : Un état d'esprit

Compléter le raisonnement fonctionnel avec l'approche sécurité (duale)

- fonctionnel : trouver une solution apportant les services attendus
- sécurité : interdire ce qui n'est pas autorisé, prendre en compte le dysfonctionnel, identifier l'imprévu, *etc.*

En évitant les confusions entre sûreté de fonctionnement et sécurité...

Promouvoir aussi des concepts tels que la défense en profondeur et ses 5 axes

- Prévenir
- Limiter
- Réparer
- Bloquer
- Détecter

Enseigner la SSI : Défensif vs offensif

Les formations en SSI comportent souvent une partie offensive

- nécessaire à la sensibilisation et utile à la compréhension
- souvent assez facile, visuel. . . et très « vendeur »

Pour autant

- connaître l'offensif ne donne pas (toujours) les moyens de protéger ou défendre
- les limites juridiques sont-elles connues et respectées ?
- risque de dérive, la sécurité par *patches*

La juste répartition devrait découler des objectifs métier

Enseigner la SSI : Largeur vs profondeur

Des sujets incontournables dans une formation en SSI ?

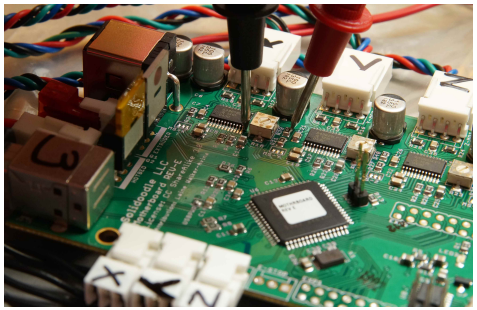
Surtout un besoin de cohérence ! Un spécialiste SSI formé à un outil doit en comprendre toutes les forces et faiblesses

Quelques exemples élémentaires

- cryptographie : primitives, formats, modes, protocoles, génération de clés, architecture de clés, implémentations (*bugs*, canaux auxiliaires), aspects organisationnels (IGC), lois...
- applications *web* : architecture réseau, installation des serveurs, configuration des services, structure et rôles de la base de données, développement robuste, filtrage des données utilisateur...

Enseigner la SSI : Technique vs normes

La SSI, c'est bien sûr de la technique, mais c'est aussi



- de l'humain et de l'organisationnel
- du juridique et du réglementaire
- de la méthodologie et des normes
- ...

Le tout technique n'est pas forcément approprié... mais le sans technique non plus ; la répartition appropriée fait souvent la part belle à la technique