PROTECTION DES INFRASTRUCTURES CRITIQUES

Approches physique et cyber

Séminaire d'information Horizon 2020
Lundi 18 mars 2019

–

Secrétariat général de la défense et de la sécurité nationale

SGDSN

Qu'est-ce qu'une **activité d'importance vitale ?**

Une activité « dont l'indisponibilité risquerait de diminuer d'une façon importante le **potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation. »**

(extrait de l'article L. 1332-1 du code de la défense)

Les établissements « dont la destruction ou l'avarie [...] peut présenter un **danger grave pour la population**. »

(extrait de l'article L. 1332-2 du code de la défense)

SGDSN

Qui est **concerné ?**

un opérateur

PUBLIC ou PRIVE

Ex : une institution, un site de production, un centre de contrôle ou un data center.

SGDSN

12 secteurs d'activités d'importance vitale

DOMINANTE REGALIENNE

- Activités civiles

- Justice

- Activités militaires

DOMINANTE HUMAINE

- Alimentation

- Eau

- Santé

DOMINANTE ECONOMIQUE

- Énergie

- Transport

- Finance

DOMINANTE TECHNOLOGIQUE

- Industrie

- Communications électroniques et audiovisuel

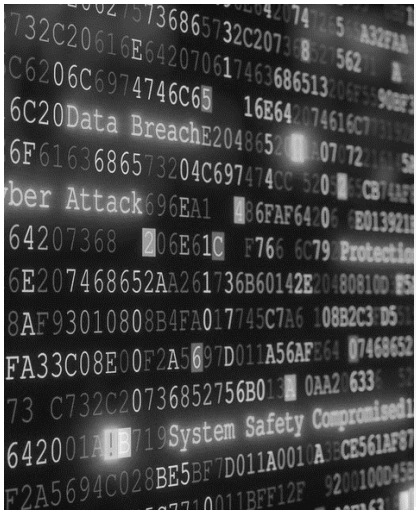
- Espace & recherche

SGDSN

Quels sont **les risques et les menaces ?**

« […] un acte de **malveillance, de sabotage ou de terrorisme** »

(extrait de l'article R. 1332-1 du code de la défense)



Depuis 2013

Tous les risques auxquels sont potentiellement exposés les opérateurs (risques naturels, technologiques, sanitaires etc.).

SGDSN

Quelles sont les **obligations ?**

« Les opérateurs publics ou privés [d'importance vitale] sont tenus de **coopérer à leurs frais** [...] à la protection [des sites qu'ils exploitent] contre toute menace, notamment à caractère terroriste. »

(extrait de l'article L. 1332-1 du code de la défense)

SGDSN

Le processus de **planification**

PLAN VIGIPIRATE

GESTION DE LA MENACE

12 **secteurs opérateurs**

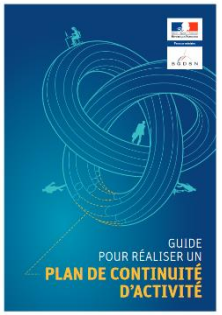
directive nationale de sécurité (DNS) pour chaque secteur d'importance vitale

GESTION DES RISQUES

250

plan de sécurité opérateur (PSO)

+ CONTINUITÉ D'ACTIVITÉ



pour chaque point d'importance vitale (PIV)

>1500 **PIV**

plan de protection particulier (PPP) ⟷ plan de protection externe (PPE)

Mode d'emploi = instruction générale interministérielle 6600 du 7 janvier 2014

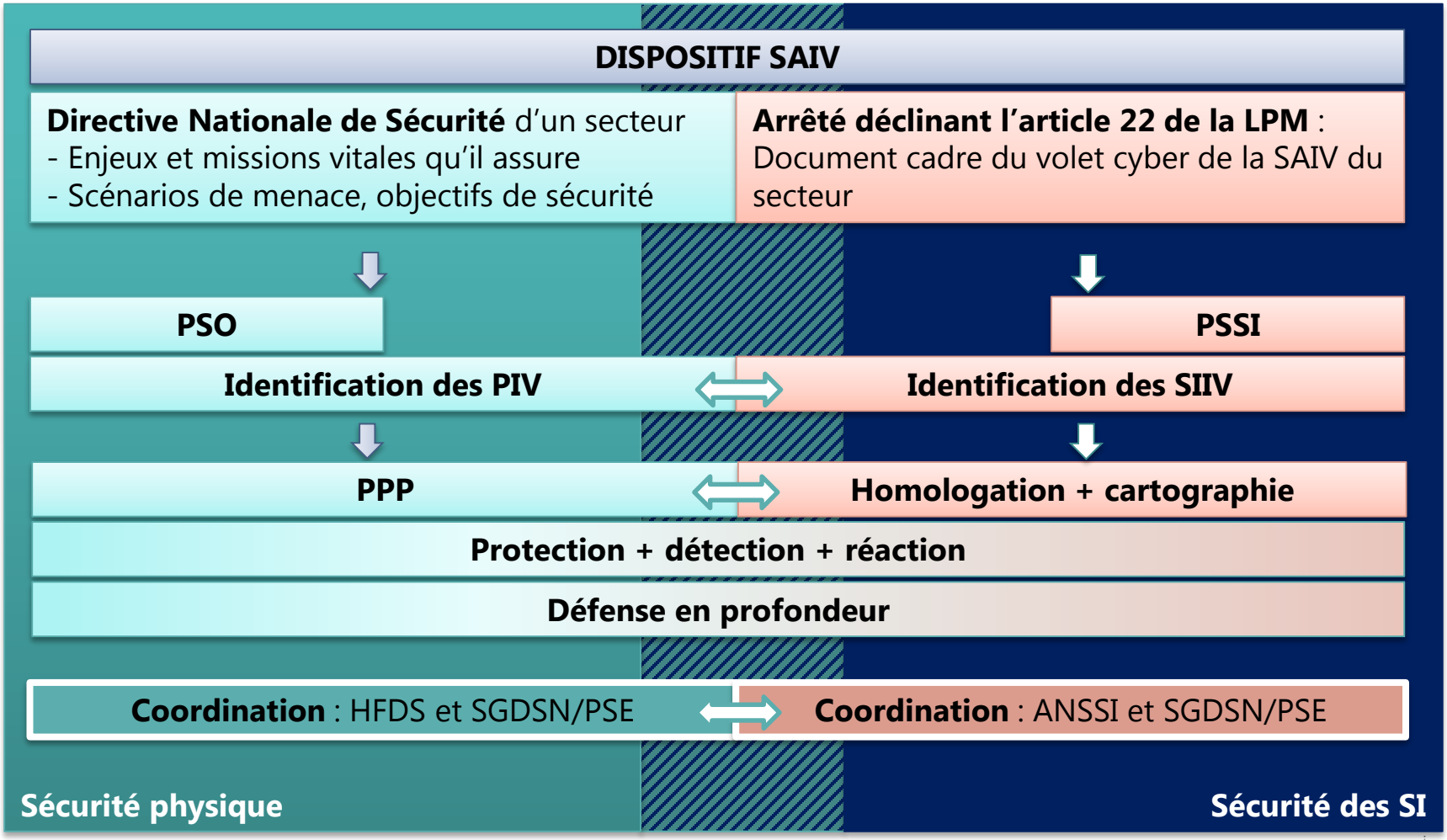
SGDSN

Bilan du dispositif

- Des OIV clairement identifiés
- Moyens et services de l'Etat mobilisés
- Un seul point de contact : le délégué pour la défense et la sécurité
- Partage d'information sur l'évaluation de la menace - VIGIPIRATE
- Une homogénéisation du niveau de protection
- Acteurs plus mobilisés et sensibilisés

SGDSN

Le volet **cyber** de la SAIV



SGDSN

Le volet **cyber** de la SAIV

> Articulation sécurité et SSI : l'un ne va pas sans l'autre !

> Articulation SSI et systèmes industriels (automaticiens)

> Identification des SIIV : exploration des processus métiers pour y déceler ce qui est vital – en lien avec les missions d'importance vitale

> Sensibilisation des sphères privée et public

> **Augmentation du niveau de cybersécurité des OIV, des prestataires et, par diffusion, des autres entités**

SGDSN

Le volet cyber de la SAIV – l'action de l'ANSSI

> Rencontres, sensibilisation, assistance technique, aide à la réponse aux incidents

> CERT-FR : collecte d'incidents, veille sectorielle et multi-sectorielle, campagnes de marqueurs

> Actions génériques : notes techniques, guides (homologation, systèmes industriels), développement de l'offre technologique, labellisation de prestataires et de fournisseursc

SGDSN

Le volet cyber de la SAIV – **4 piliers**

> Préalable : identifier les systèmes d'information d'importance vitale (SIIV)

> 4 piliers :
- Règles s'appliquant sur les SIIV : organisationnelles, gouvernance, préventives et réactives
- Déclaration des incidents SSI à l'ANSSI
- Contrôles par l'ANSSI ou un prestataire d'audit SSI qualifié par l'ANSSI
- Le Premier ministre peut imposer sur proposition de l'ANSSI des mesures cyber aux OIV en cas de crise cyber majeure

SGDSN

La Directive NIS

Objectif :
Assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne

Renforcer les capacités nationales des États membres en matière de cybersécurité :
Un cadre de gouvernance commun

Mise en place d'une coopération entre les États membres

Instauration d'un cadre réglementaire destiné à renforcer la cybersécurité des fournisseurs de service numérique qui sont essentiels au fonctionnement de l'économie et de la société (FSN)

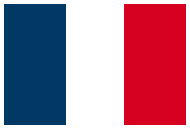
Instauration d'un cadre réglementaire destiné à renforcer la cyber sécurité des opérateurs de services qui sont essentiels au fonctionnement de l'économie et de la société (OSE)

➡ Articulation NIS /SAIV

Le programme européen de protection des infrastructures critiques

Directive 2008/114/CE

- 2 secteurs : énergie, transports
- Infrastructure critique européenne
- Plan de sécurité d'opérateur
- Correspondant pour la sécurité



Code de la Défense (SAIV)

- 12 secteurs
- Point d'importance vitale
- PSO ou PPP
- Délégué pour la défense et la sécurité

• Equivalence des plans entre les deux dispositifs

• Pas d'autres référentiels que les DNS

• Pas de contrainte supplémentaire pour les opérateurs

• Identification des ICE françaises suite discussions bilatérales avec les Etats voisins

•2019 : révision de la directive ?

SGDSN

Le programme européen de protection des infrastructures critiques

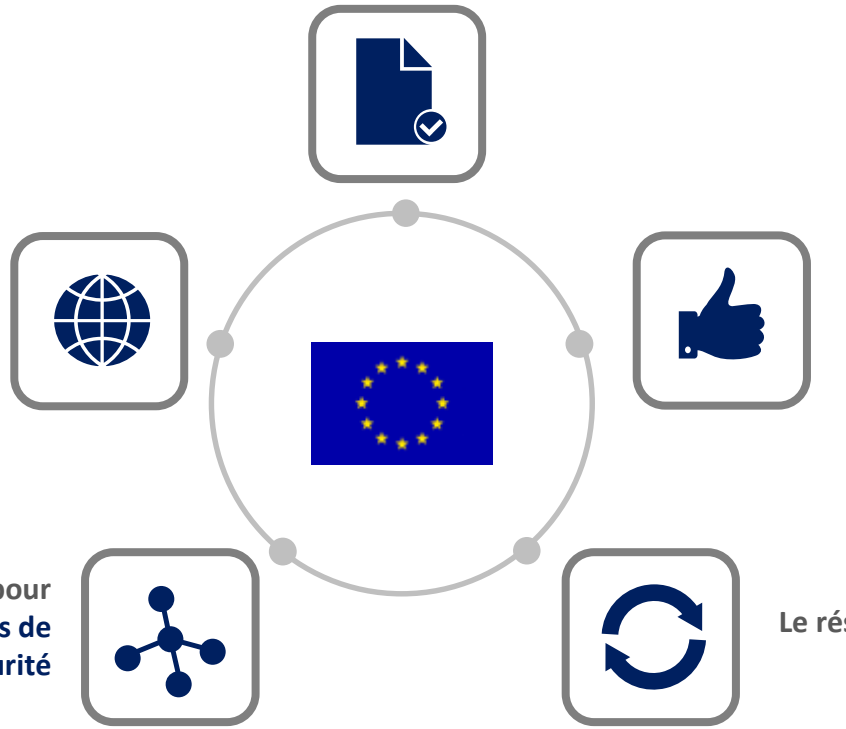
La **directive** du Conseil du 8 décembre 2008 : infrastructures critiques européennes

La politique envers les **Etats tiers**

Soutien de la **Commission** aux Etats membres

Le **réseau européen de référence** pour l'expérimentation de **solutions de sécurité**

Le réseau d'information **CIWIN**



SGDSN

Genèse et place dans le **PCRD**

- Protection des infrastructures critiques : **une des quatre missions principales identifiées dès 2006 dans les travaux de l'ESRAB.**

- 7ème PCRD – Sécurité (2007-2013)
  - Périmètre CIP hors cyber
  - 55 projets financés pour 259 M€ de subventions

- Horizon 2020 – Défi société sûres
  - Position française pour une **approche intégrée protection physique et digitale**
  - depuis 2016, un call spécifique et commun entre la DG HOME et la DG CNECT

SGDSN

COORDONNÉES

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET
DE LA SÉCURITÉ NATIONALE

Direction de la protection et de la sécurité de l'Etat
Agence nationale de la sécurité des systèmes d'information

http://www.sgdsn.gouv.fr/
https://www.ssi.gouv.fr/