Les réponses et remèdes apportés par l’État jusqu’aux années 2000

Joël Hosatte

Les années 1950

- Les apports du projet MYOSOTIS (1963)
  - Créer une industrie du chiffre souveraine
  - Définir la doctrine du chiffre gouvernemental
  - Constituer une école du chiffre

- Quelle est l'organisation de l'État ?

Armement (fin des années 50)

- Secrétaire d'État Terre : Direction des études et fabrication d'armement - DEFA
- Secrétaire d'État Mer : Direction centrale des constructions et armes navales - DCCAN
- Secrétaire d'État Air : Direction technique et industrielle de l'aéronautique - DTIA
- Poudres : Direction des poudres

Dès 1954, début des études de l'arme nucléaire et étude de missiles dans le cadre OTAN

5 avril 1961 – Délégation ministérielle pour l'Armement

- 4 directions : DEFA, DCCAN, DTIA, Poudres
  + DRME (Recherche et Moyens d'Essais)
- 8 départements de coordination : Engins
  Atome (armes restent CEA/DAM)
  Électronique : télécommunications et radar
  Administration, Expansion Économique, etc.
- mission : force nucléaire et programmes d'armement
- DEL → SCTI avec création du CELAR (1968),
  → DEI (1982) avec STEI et CELAR (DGA/MI)

Organisation interministérielle

- 1951 Commission interministérielle des chiffres
  STCCh : Service technique central des chiffres, rattaché au Premier ministre (SGG)

- 1958 : atelier de fabrication de bandes perforées aléatoires, pour les équipements TAREC Translation Automatique Régénératrice Et Chiffrante

- CECS : Centre d'études cryptographiques supérieures, rattaché en 1962 au STCCh

B211 et C36 en service en 1956

1956 - Crise du canal de Suez

Gamal Abdel Nasser

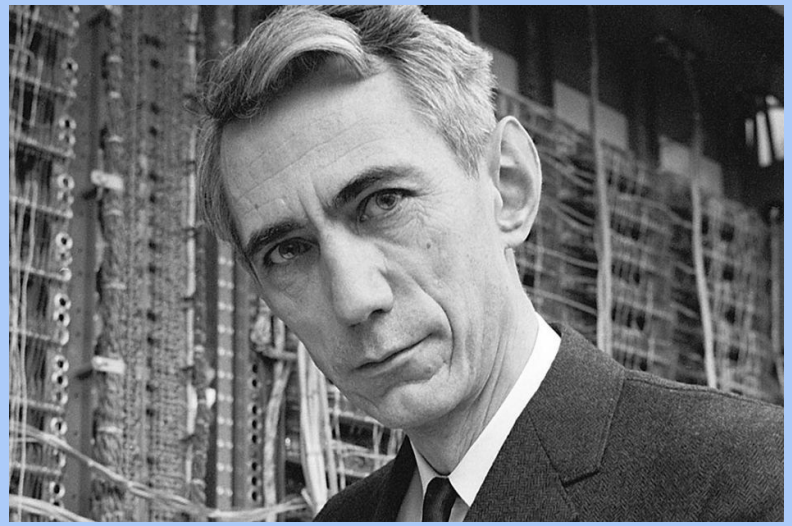
- Refus US et URSS de financer le barrage d'Assouan :
  - 26 juillet : le président Nasser nationalise le canal de Suez
  - F et UK, cogestionnaires du canal réagissent
  - Accord secret F, UK, Israël et intervention militaire

- Vos B 211 sont vulnérables

Le projet MYOSOTIS

- Ulysse (Marine)
- Violette (Air) – Sagem
- Myosotis (Terre) – CSF
- Concours OTAN
  - Évaluation opérationnelle : Shape Rocquencourt
  - Évaluation de sécurité : SECAN (NSA)
  - Approbation pour tout niveau de classification
- Tensions avec les US précédant notre retrait en 1966 de l'organisation militaire intégrée

La base de notre monde numérique



Claude Shannon

- Sigsaly : cryptophonie Roosevelt - Churchill
- *A mathematical theory of communication*
  1948 Journal Bell
  1949 Livre
- *Communication theory of secrecy system*
  1945 Classifié
  1949 Version non classifiée

L’évaluation de Violette et Myosotis

- Chiffre incassable (Shannon) = Système de Vernam (masque jetable) avec une clé aléatoire aussi longue que le message.
- Constitution d’une équipe : STCCh A. Müller – Col Cattieuw
  J. R. Barra Définition des tests statistiques
- Transcient ElectroMagnetic Pulse Emanation Standard - Signaux parasites compromettants
- APREDOSTAT (1968)
  Fétiche (RITA) – Cryptomod (TM 30, Capucine)

Les apports du projet MYOSOTIS

- Doter la France d'une industrie du chiffre souveraine : Thomson-Csf et Sagem
- Définir la doctrine du chiffre gouvernemental en conception, évaluation et emploi
  I. I. 500/STCCh du 23 décembre 1968
  I. I. 300/STCCh du 7 avril 1973 (TEMPEST)
- Constituer une véritable école du chiffre
  CECS → CFSSI

La sécurité informatique en 1980

- Sécurité physique des locaux
- Habilitation des personnels
- Chiffrement des données transmises

- Multi tâches ; déport des terminaux
- Besoin de mécanismes de sécurité
- Monde nouveau pour les informaticiens
- Groupe de coordination SSI
  interne DGA + DCT (Terre) + SERTIM (Marine)

Création du SCSSI le 3 mars 1986

- Besoin de renforcer les effectifs du STCCh
- Les dirigeants ignorent tout du domaine
- Réflexion pilotée par la Défense → 3 mars 86

  décret 317 : Délégation interministérielle SSI
  décret 318 : Service central de la SSI
  décret 319 : Centre de formation SSI

- Fusion Sécurité informatique et Chiffre
- DCSSI (2001) et ANSSI (2009)

Le processus d'homologation

- Sécurité = Confidentialité, mais aussi Disponibilité et Intégrité/authenticité.
- 3 intervenants :
  - Commanditaire précise la cible d'évaluation TOE et la cible de sécurité
  - Évaluateur indépendant
  - Organisme de certification
- 2 assurances : efficacité (E1 à E6) et conformité

Élaboration des critères d'évaluation

- Précurseur : livre orange TCSEC (US DOD 1983)
  Trusted Computer Systems Evaluation Criteria
- Réticence d'une application du processus à l'OTAN
- CESG Memorandum n°3 de janvier 1989
- ZSIEC Livre vert allemand de janvier 1989
- Livre Bleu Blanc Rouge n°692/SGDN/DISSI/SCSSI de juillet 1989
- Concept valable pour gouvernemental et commercial

Les ITSEC puis les Critères communs

- F, UK, D et NL ont la volonté
  - d'harmoniser les critères d'évaluation
  - d'aboutir à la reconnaissance mutuelle des certificats (demande forte des industriels)
- Vaste consultation internationale sous l'égide de la commission de l'Union européenne
  Publication des ITSEC V2 en juin 1991
- Discussion à l'ISO pour des critères uniques

SCSSI / Industrie française

- Trouver les acteurs pour faire vivre le processus d'homologation
- Disposer d'évaluateurs indépendants, viables économiquement et accrédités par le COFRAC
  Carte à puce : Service d'études communes de la Poste et de France Télécom (SEPT) à Caen
- Inciter les fournisseurs à se faire certifier

SCSSI / Ministères

- Une des missions : évaluation des systèmes d'information gouvernementaux
- Dialogue : - mon système est-il sûr ?
  - pour quel besoin et quel emploi ?
- FEROS : Fiche d'Expression Rationnelle des Objectifs de Sécurité
- EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité
- CERT-A

Merci de votre attention