La légitime défense des réseaux

Modélisation
et paramètres juridiques

David BENICHOU

Serge LEFRANC

MINISTÈRE DE LA DÉFENSE

DGA

Légitime défense des réseaux

Introduction

- **La problématique de départ**
  - ➔ Quelles sont les conditions de la légitime défense des réseaux ?

- **L'hypothèse de départ**
  - ➔ Dans le monde réel, le pire n'est jamais certain…

Légitime défense des réseaux

Prolégomènes

- **Le droit de la guerre** ne connaît pas la guerre de l'information (la doctrine, oui).
- **Le droit commun** ne connaît pas la guerre de l'information.
- **Faute de convention internationale, de loi ou règlement, l'exception « *d'autorisation de la loi* » serait inopérante** à exonérer les auteurs d'un acte *d'infoguerre* de leur responsabilité pénale.
  - Art. 122-4 du CP : N'est pas pénalement responsable la personne qui accomplit un acte prescrit ou autorisé par des dispositions législatives ou réglementaires.

Légitime défense des réseaux

Notions de légitime défense

- **Une règle universelle et sans âge**
  - *Non scripta sed nata lex* (Cicéron, dans Pro Milone).

- **Fondée sur 2 types de justifications**
  - Subjectives : instinct de préservation.
  - Objectives : suppléance privée du défaut de sécurité publique (*la légitime défense, défend l'ordre public*).

- **Encadrée très tôt**
  - La loi des 12 tables de la Pax Romana distingue l'attaque de jour, de l'attaque de nuit (cas d'attaque).
  - La loi du Talion, loi de modération inscrit la proportionnalité…(types de réponse).

Légitime défense des réseaux

Les conditions juridiques de la légitime défense

- **Article 122-5 du code pénal**
  - N'est pas pénalement responsable la personne qui, devant une **atteinte injustifiée** envers elle-même ou autrui, accomplit, **dans le même temps**, un acte commandé par la **nécessité** de la légitime défense d'elle-même ou d'autrui, **sauf s'il y a disproportion** entre les moyens de défense employés et la gravité de l'atteinte.
  - N'est pas pénalement responsable la personne qui, pour interrompre **l'exécution d'un crime ou d'un délit contre un bien**, accomplit un acte de défense, autre qu'un homicide volontaire, lorsque cet acte est **strictement nécessaire** au but poursuivi dès lors que les moyens employés sont **proportionnés** à la gravité de l'infraction.

Légitime défense des réseaux

Eléments constitutifs de la légitime défense

- **Une agression**
  - **Réelle** quant à son contenu et son objet.
  - **Actuelle** c'est-à-dire en cours.
  - **Injuste**: qui n'est pas ordonnée par la loi.

- **Une riposte**
  - **Simultanée.**
  - **Mesurée** (strictement proportionnée) pour les biens.

Légitime défense des réseaux

Importance de la nature de l'intérêt protégé

- **Défend-on des biens ou des personnes ?**
  - Un système d'information est un ensemble **de biens**…qui peut être le support de données **personnelles**…qui peut être un élément essentiel d'un système de **protection des personnes** (infrastructures vitales…).
  - Enjeu: des régimes juridiques différents (122-5 al 1 ou 2).

Défense des PERSONNES	Défense des BIENS
« commandé par la nécessité »	*« strictement nécessaire »*
L'accusation doit faire la preuve de la disproportion	*Le défenseur doit faire la preuve de la proportion (homicide toujours exclu)*

Légitime défense des réseaux

Nécessité de la réponse automatique

- La réponse de nature humaine, dans un environnement d'attaque en réseau ne paraît pas susceptible d'être réalisée dans le temps de l'attaque (sauf pour une attaque qui dure, type déni de service). La réponse humaine suppose en effet des actes longs (identification des traces, élaboration d'une décision).

- Pour satisfaire aux conditions de **simultanéité** et de **proportionnalité**, la défense des réseaux doit reposer, ***a minima***, sur des mécanismes de **réponses automatiques graduées**.

Notre modèle: le SRA

- **SRA = Système de Réponse Automatique**
- **2 niveaux de menace**
  - Les menaces sont prédéfinies et classées en « événements hostiles ».
- **3 niveaux de réponse**
  - La réponse est paramétrée.

Événements hostiles	Contre-mesure	Qualifications pénales (art. 323-1 et suivants du code pénal)
1. Prise d'empreinte	**1.** Archiver et traiter	/
2. Paquet d'attaque	**2.** Déni de service	**Délits** d'entrave au fonctionnement et/ou d'accès frauduleux aggravé (modification de données)
	3. Attaque	

- **Exemple**
  - Si 1 alors riposte 1.
  - Si 2 alors riposte 2 ou 3 en fonction du paquet.

Légitime défense des réseaux

Démonstration

- **Le modèle est universel**
  - Quelque soit la sophistication du procédé, le fonctionnement peut-être ramené au modèle primaire.

- **Mise en situation**
  - Vous êtes responsable d'un établissement de niveau 1, ouvert sur le monde extérieur. Convaincu de l'intérêt d'une telle solution présentée lors d'un salon sur la sécurité, vous avez déployé un système de réponse automatique…

- **Mardi 10 mai 2005…peu avant la pause déjeuner…**

Légitime défense des réseaux

Démonstration

- **Ce que la victime voit…**

Légitime défense des réseaux

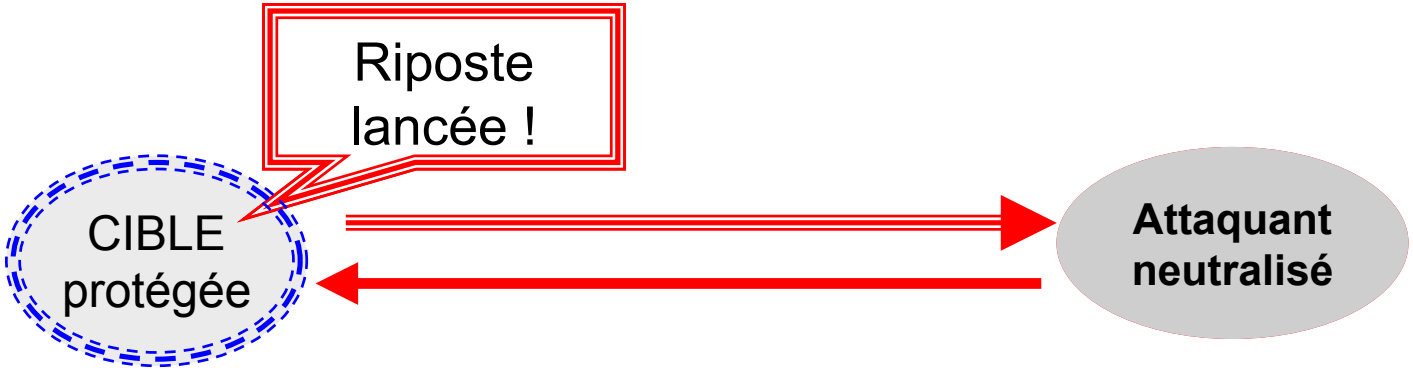
Débriefing

- **Ce qui s'est réellement passé derrière le réseau de la victime correspond à 3 scénarios possibles (au moins)**
  - La réponse du SRA est réductrice.
  - Unique, elle répond indifféremment à trois situations différentes.

Légitime défense des réseaux

Scénario 1: l'attaque imprudente ou kamikaze

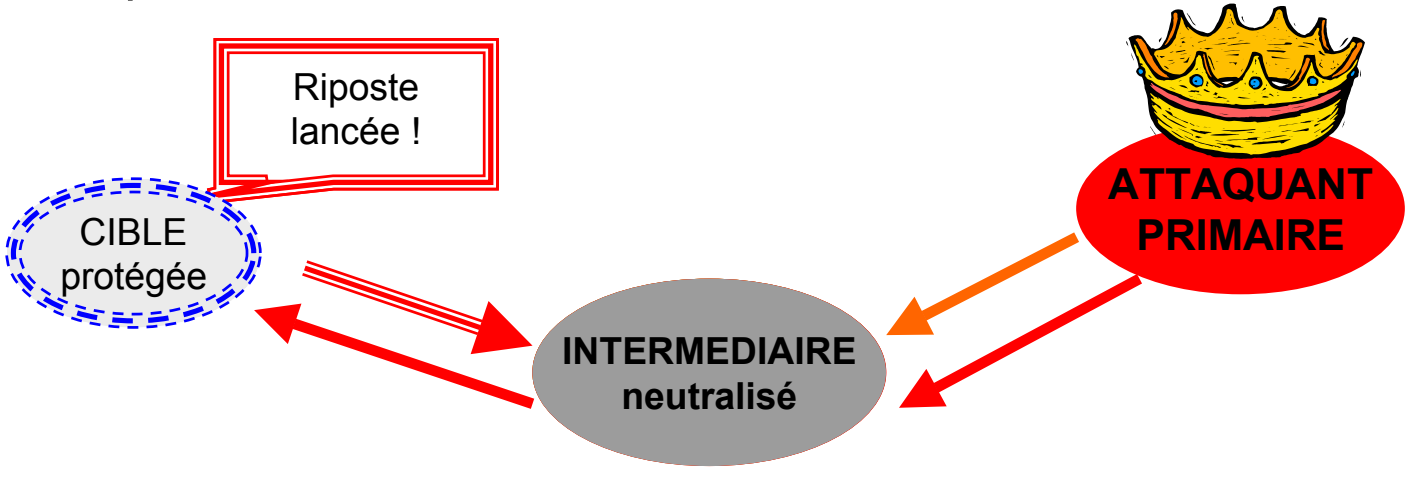
- **Le pirate attaque sa cible à partir de sa propre machine**
  - La cible est capable de connaître l'adresse IP de l'attaquant de façon certaine et immédiate.
  - Les mécanismes de contre-mesures vont être capables de répondre efficacement à cette attaque, il n'y a pas d'ambiguïté.



Légitime défense des réseaux

Scénario 2: l'attaque prudente

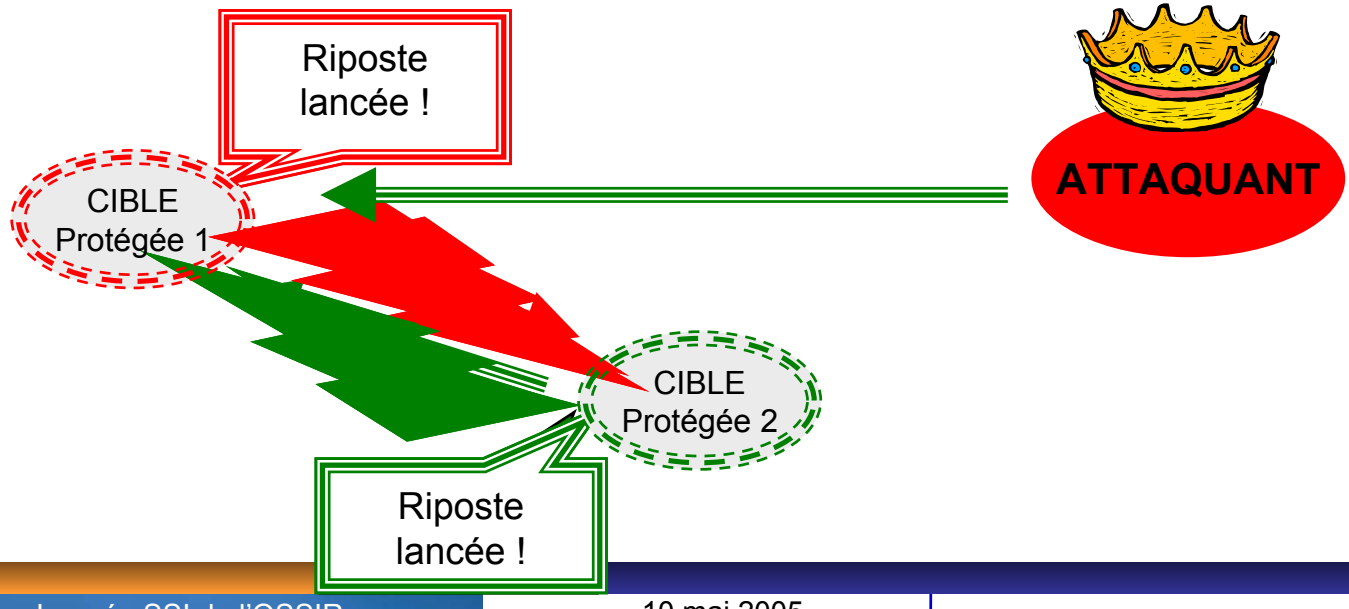
- **Le pirate lance l'attaque à partir d'une machine qu'il a compromise**
  - Il est possible d'identifier la provenance physique de l'attaque, mais cela ne donne pas d'indication sur le véritable instigateur du piratage.
  - Les mécanismes de contre-mesures ne vont pas être capable de répondre efficacement.



Légitime défense des réseaux

Scénario 3: l'attaque astucieuse

- **Le pirate lance l'attaque en utilisant une adresse source usurpée: son but créer un conflit entre deux entités**
  - Cette situation suppose que la cible primaire et la cible secondaire soient toutes deux dotées de SRA (sites sensibles)…
  - Les deux cibles vont se détruire mutuellement, d'une manière automatique, le vrai agresseur n'a qu'à envoyer le 1er paquet.



MINISTÈRE DE LA DÉFENSE
DGA

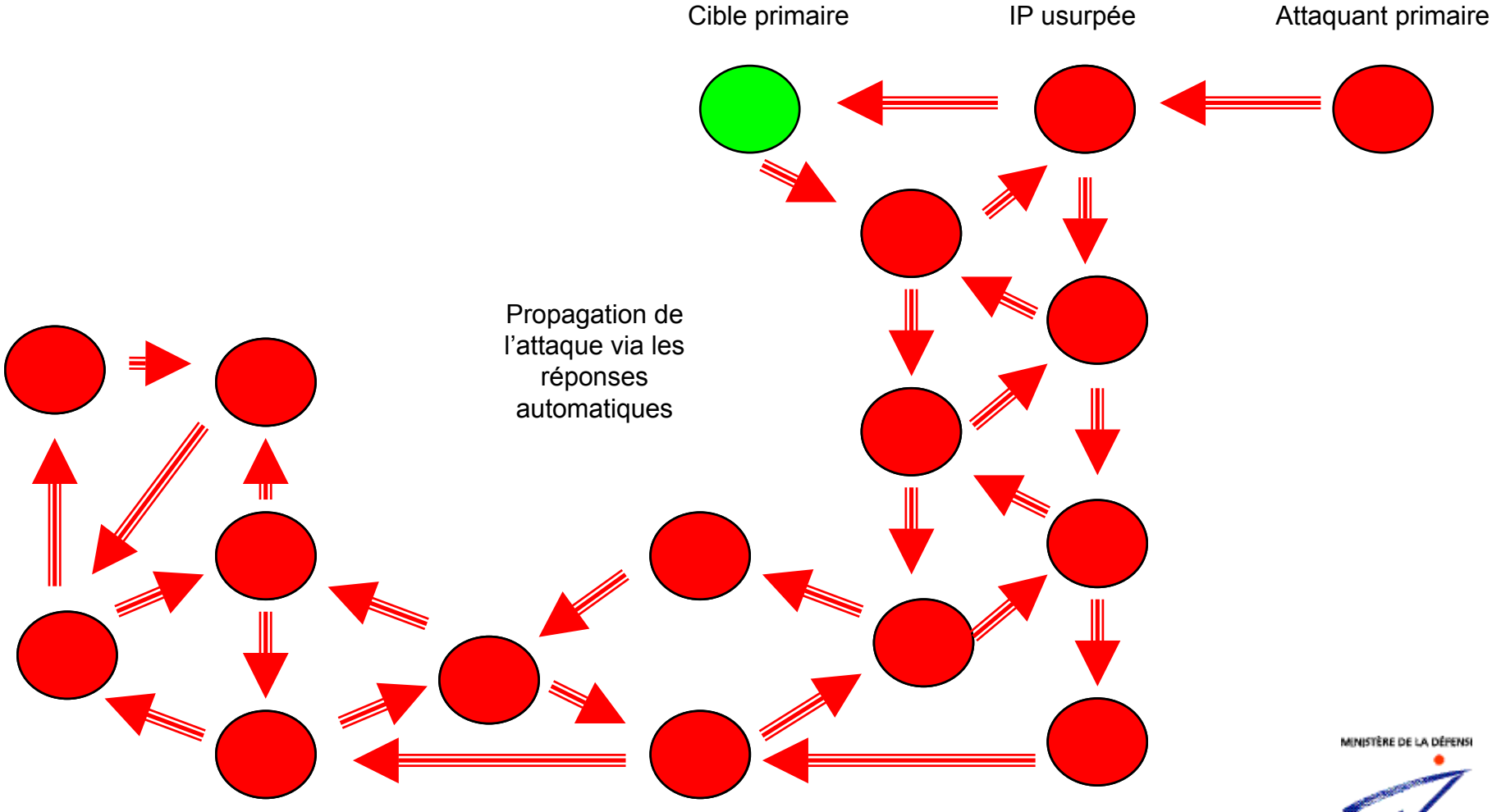
Légitime défense des réseaux

Une réaction en chaîne probable…

- **C'est l'hypothèse d'une réaction en chaîne si les SRA utilisent pour leur attaque une usurpation d'adresse IP:**
  - Il existe une probabilité que la machine usurpée soit elle-même dotée d'un SRA, recevant la contre attaque elle mettra en œuvre sa contre mesure, en utilisant elle-même une usurpation d'IP et contre une machine dont l'adresse aura été usurpée…
  - Si la présence de SRA usurpant l'adresse source d'une machine elle-même dotée d'un SRA, dépasse un certain facteur, on peut assister à une réaction en chaîne…

Légitime défense des réseaux

La réaction en chaîne



MINISTÈRE DE LA DÉFENSE
DGA

Légitime défense des réseaux

Bilan

- **A l'heure actuelle il est très difficile, parfois impossible d'identifier avec certitude l'origine réelle d'une attaque informatique**

NIVEAU D'ATTAQUE	RISQUES entraînés par la riposte	GAINS
3: Astucieuse	**1. Être l'auteur manipulé de l'attaque** **2. Plaintes réciproques** **3. Imbroglio diplomatique et/ou institutionnel au niveau politique**	**0**
2: Prudente	**1. Se tromper de cible** **2. Poursuites judiciaires civiles ou pénales, condamnation probable**	**0**
1: Imprudente	Poursuites judiciaires improbables (sauf si la réponse a été inadaptée)	Neutralisation temporaire de l'attaquant possibilité de poursuite judiciaire

Légitime défense des réseaux

Conclusion

- **Dans le monde réel, le pire n'est jamais certain…mais avec la légitime défense des réseaux préparez vous au pire !**
- **Avons-nous besoin d'un régime juridique pour la guerre de l'information et la protection des infrastructures vitales ?**
- **Piste de la défense en profondeur…**

David Bénichou (juge d'instruction)
David.Benichou@justice.fr

Serge Lefranc (ingénieur de l'armement)
serge.lefranc@dga.defense.gouv.fr

MINISTÈRE DE LA DÉFENSE
DGA