"Les cybermenaces à l'horizon 2020"

Les enjeux du cyberespace

par le Général d'armée
Marc WATIN-AUGOUARD
Inspecteur général des armées - gendarmerie

Présentation des résultats de l'étude prospective sur la cybercriminalité 2011-2020

Introduction et méthodologie

Email : guinier@acm.org

par Daniel GUINIER

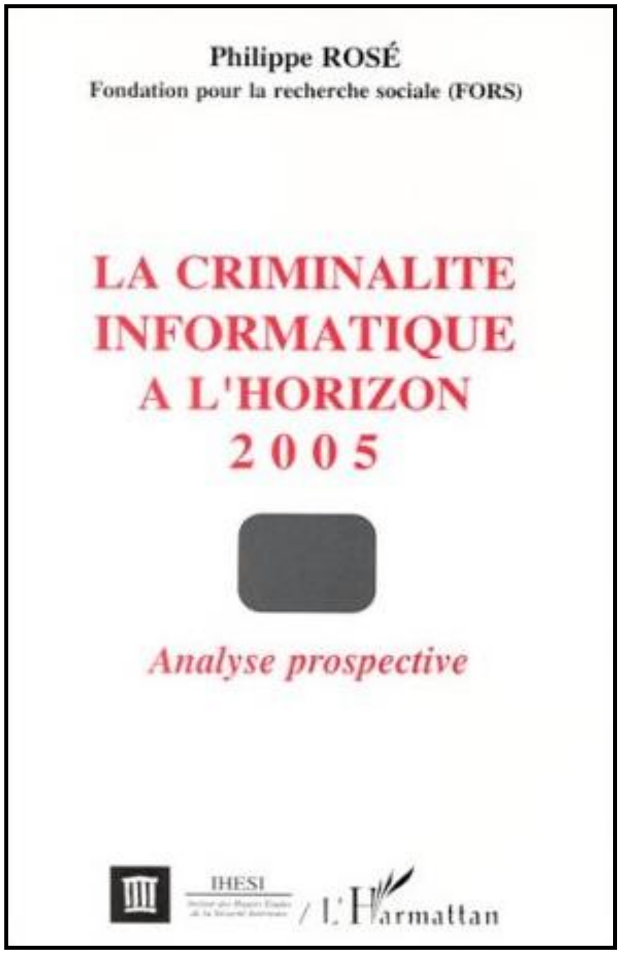
Dr. ès Sciences, Certifications CISSP, ISSMP, ISSAP, MBCI

Expert judiciaire honoraire près la Cour d'Appel de Colmar

Expert devant la Cour Pénale Internationale de La Haye

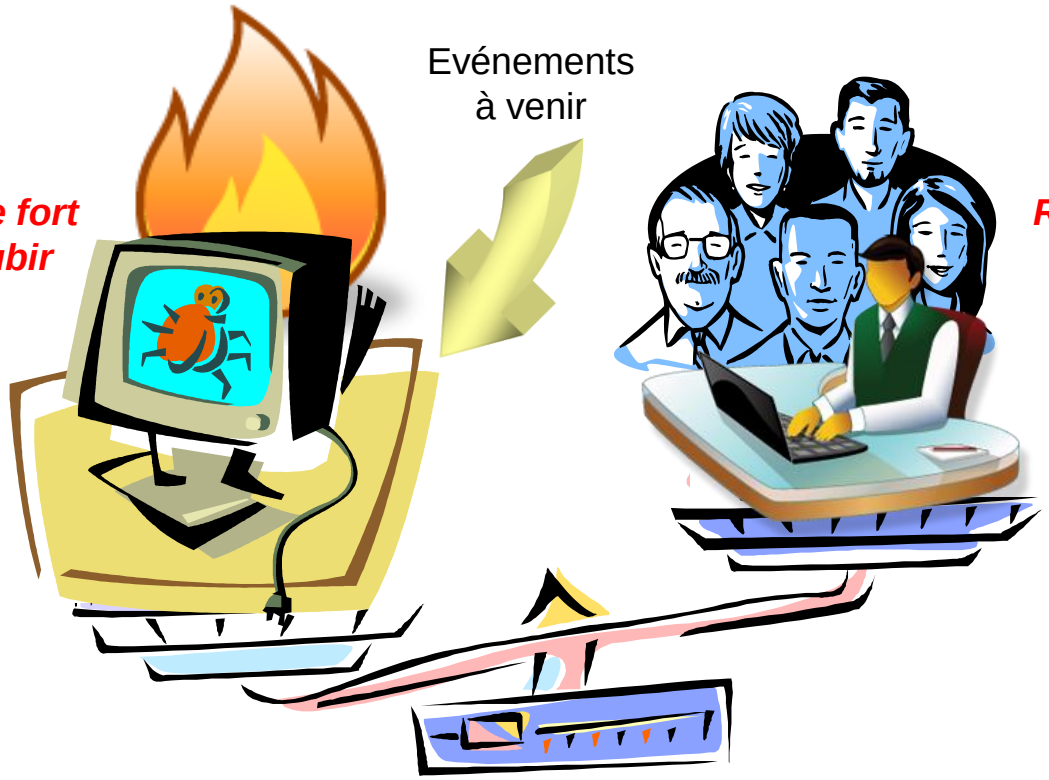
Lieutenant-colonel (RC) de la gendarmerie nationale

Une prospective pour mieux anticiper



La prospective réussie de 1991 à 2005, malgré les ruptures technologiques, justifiait un renouvellement pour 2011 à 2020.

Le dilemme relatif au futur



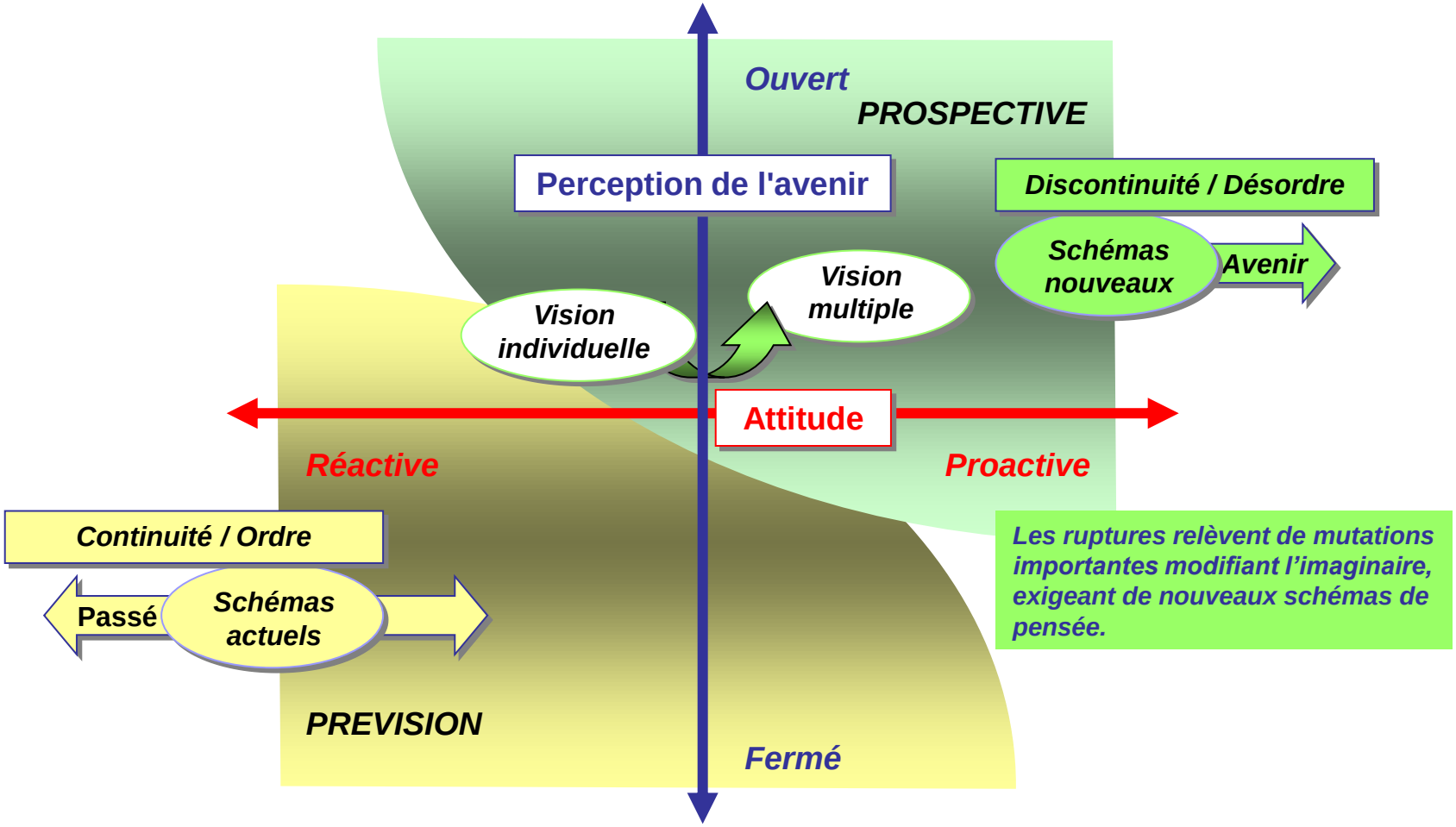
Attitude passive ➡ Situation de faiblesse

Attitude active ➡ Situation de force

Général Marc WATIN-AUGOUARD - Préface

"Qui tente de prévoir l'avenir, prend le risque de se tromper. Qui néglige la prospective adopte une attitude passive qui le place en situation de faiblesse face à la dictature des événements".

Choix de l'approche prospective



La discontinuité impose l'approche prospective coopérative pour des schémas nouveaux, plutôt que l'anticipation par la prévision fondée sur la continuité des schémas actuels relevant du passé.

Caractéristiques de la prospective

- **Objectif** :
  - Poser les jalons d'une réflexion sur l'avenir
- **Domaine** :
  - La cybercriminalité
- **Champs** :
  - Différents axes thématiques de ce domaine
- **Buts** :
  - Identifier les points-clés du futur
  - Repérer les scénarios possibles
  - Envisager différentes ruptures

L’avenir n’est ni déterminé, ni le produit du hasard, et le devenir découle de la volonté des hommes. Ainsi, la prospective est au service des actions à mener au vu des enjeux, pour mieux le bâtir.

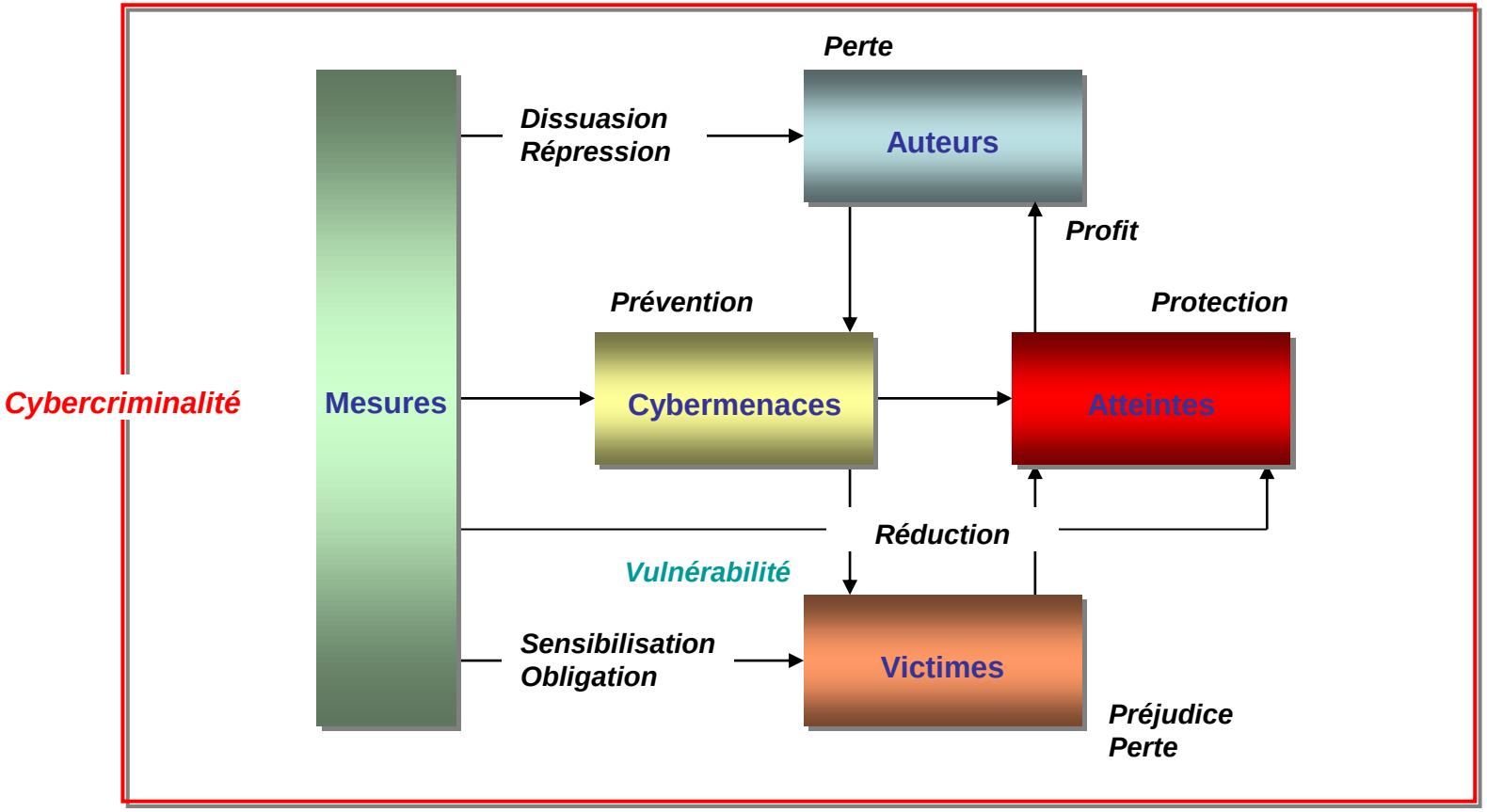
Méthode de prospective choisie

- **DELPHI** : Méthode de prospective reconnue
  - Utilisée avec succès, y compris dans ce domaine (*)
  - Questionnaire ouvert bâti autour d'axes thématiques
  - Réponses indépendantes au questionnaire
  - Réponses anonymes pour éviter l'effet de leadership
  - Processus répété sur plusieurs tours, où chacun est invité à reprendre, reformuler ou compléter ses réponses :
    - pour réduire la dispersion et préciser l'opinion médiane
    - pour provoquer la réflexion et enrichir l'information

(*) **Rosé P**. (1992) : *La criminalité informatique à l'horizon 2005 - Analyse prospective*, l'Harmattan, 165 p.

Ceci permet non seulement l'obtention d'un consensus et d'une réduction de la dispersion, mais aussi d'apporter une information plus riche, avec des opinions minoritaires mais très argumentées.

Modèle thématique systémique



Menaces : enlèvement, destruction, interruption, modification, divulgation, interception, image, etc.
Atteintes aux infrastructures, matériels, logiciels, données, à la réputation, etc.
Auteurs d'actes délictueux : cybercriminels, *"hackers"*, groupes activistes, terroristes, etc.
Victimes subissant des préjudices par l'application de menaces qui mènent à des atteintes,
Mesures visant la cybercriminalité : législatives, politiques, techniques, organisationnelles, humaines

Organisation des rôles pour l'étude

Proposition d'étude
Idée, motifs et méthode

Questionnaire : questions ouvertes mais précises, relevant du **modèle** thématique, réponses exigeant une argumentation

Critères de choix des experts : compétences, expérience, capacité de prévision, indépendance, pour disposer d'un panel de 20 à 30 personnes

Comité scientifique

Comité de rédaction de synthèse

23 questions :
3 générales
4 sur 5 thèmes

Experts

cyber-enquêteurs, experts SSI, spécialistes

Composition : 4 personnes

Mission : validation de la méthode, recherche des experts, rédaction et validation du questionnaire ouvert, soumission aux experts par courriel, validation du document final

Composition : **3** personnes

Mission : rédaction de la synthèse suite au recueil anonyme des réponses, à chacun des trois tours, renvoi de la synthèse par courriel pour les 2° et 3° tours

Composition : **22** personnes

Mission : réponse aux questions ouvertes, avec mention du niveau de compétence, renvoi par courriel

Le questionnaire a été élaboré sur la base du modèle thématique, par les membres du comité scientifique, puis synthétisé en retenant les questions considérées comme les plus pertinentes.

Echéancier et phases de l'étude

1.- Phase préparatoire

Lancement

04/2010 — Identification d'un **panel d'experts francophones européens**, avec leur **engagement formel** sur les échéances et accord sur la méthode

05/2010

07/2010 — **Réalisation du questionnaire Envoi** aux experts par courriel

2.- Phase de déroulement

08-10/2010 — 3 tours — 01-03/2011

11-12/2010

Disposition et **exploitation** des réponses, **renvois des synthèses**

1° tour : le questionnaire est transmis aux experts en précisant l'objet, la méthode, les conditions pratiques, le délai de réponse, l'anonymat, etc.

2° tour : chaque expert dispose de réponses anonymes sous forme synthétisée pour formuler sa nouvelle réponse ou préciser la précédente, en estimant une nouvelle fois sa capacité de jugement pour chaque question

3° tour : chaque expert est appelé à donner sa réponse définitive, et à commenter les arguments déviants, au vu d'une opinion consensuelle ou non

La durée totale de l'étude aura été de 12 mois

3.- Phase de finalisation

04/2011 — Reprise avec corrections

07-08/2011 — Reprise avec mise en forme et préface

11/2011 — Présentation et diffusion

L'étude s'est déroulée sur un an, avec des échanges exclusivement sous forme de courriels, sans générer de coût, avant sa finalisation en vue de sa diffusion.

Conclusion

"Les prévisions sont difficiles, surtout lorsqu'elles concernent l'avenir" (Pierre DAC) … Néanmoins :

- Ce travail de prospective a réuni un panel diversifié d'experts issus de divers secteurs
- La synthèse de leurs réponses étayées a permis de dégager les grandes tendances à venir du phénomène
- Cette étude n'est pas une fin en soi mais bien un outil destiné à alimenter la réflexion et aider à bâtir le futur
- Le document sera largement disponible sur l'Internet, dès aujourd'hui, et sa traduction en Anglais est envisagée

Une telle connaissance prospective devrait se révéler utile aux décideurs pour anticiper en constituant une force d'opposition efficiente fondée sur la communauté d'intérêts, l'harmonisation des législations, et les collaborations : transfrontières, public-privé.

Présentation des résultats de l'étude prospective sur la cybercriminalité 2011-2020

Concernant les cybermenaces

Email: dominique.schoenher@gendarmerie.interieur.gouv.fr

par Dominique SCHOENHER

Co-rédacteur de l'étude prospective

Officier-professeur
du Centre d'enseignement supérieur de la gendarmerie

Lieutenant-colonel de la gendarmerie nationale

Amplification et diversification (1/3)

- **Amplification et diversification des cybermenaces**
  - **Avis unanime des experts quelle que soit la cible**
- **Facteurs aggravants intrinsèques au cyberespace**
  - Distanciation et instantanéité facilitant le passage à l'acte (anonymat) et compliquant les poursuites/ripostes (impunité)
  - Volatilité des données et des preuves numériques (traçabilité)
  - Lacunes du droit, des moyens d'investigation et de coopération internationale
  - Espaces protégés dédiés aux activités cybercriminelles : *forums, shops, hébergeurs BulletProof (*), monnaie virtuelle, etc.*

(*) L'hébergement *"BulletProof",* ou *"à l'épreuve des balles",* indique que rien ne peut l'atteindre, simplement parce que les autorités ne peuvent intervenir pour enquêter ou fermer les serveurs. Dans ce cas, l'hébergeur offre une complaisance sur l'identité des clients, le contenu, les moyens de paiements, l'utilisation du service, etc., en plus de services usuels ou à valeur ajoutée.

"Le glaive a l'avantage stratégique sur le bouclier et cet avantage grandit".

Amplification et diversification (2/3)

- **Facteurs aggravants issus de la cible**
  - Pénétration croissante des TIC dans toute activité (+ de cibles)
  - Rythme d'obsolescence des matériels et logiciels (+ de vulnérabilités)
  - Mobilité, nomadisme et *"cloud computing"* (- de contrôle)
  - Interconnexions et interdépendances multiples des réseaux (+ de vulnérabilités)
  - Logique commerciale et productive (- de sécurité)
  - Abolition du cloisonnement des sphères professionnelle, privée et publique avec les réseaux sociaux (- de contrôle)
  - Conscience toujours insuffisante et plaintes rares

Des cibles toujours plus vulnérables.

Amplification et diversification (3/3)

- **Facteurs aggravants issus des attaquants**
  - Changement de profil *(motivation, organisation)*
  - Appropriation par le crime organisé *(rapport gain/risque, exploitation des potentialités, organisation industrielle et commerciale, blanchiment)*
  - Identification comme une arme de déstabilisation massive
  - Durcissement de l'environnement concurrentiel

Des attaquants mieux organisés et plus professionnels.

La professionnalisation

- Hier

Chen-Ing Hau,
24
(author of CIH virus)

Jeffrey Lee Parson, 18
(author of Blaster.B virus)

Joseph McElroy, 16
(Hacked into Nuclear US Lab)

- Aujourd'hui

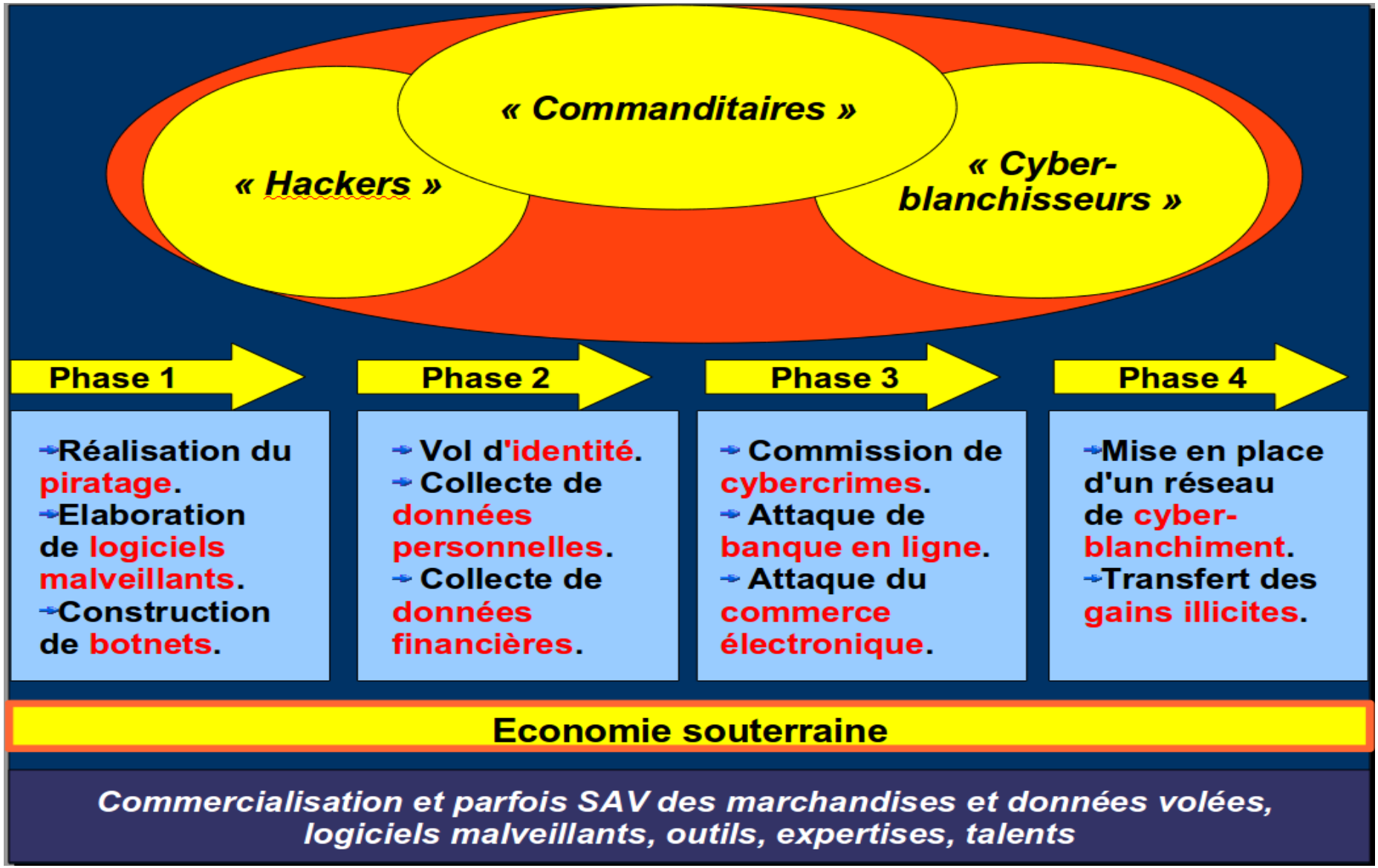
Ehud Tenenbaum
The Analyzer

Albert Gonzalez
TJX Hacker

Andrew Schwarmkoff
Russian phishing mob

Source: Présentation RSA 22/09/2011

Vers une activité de service



Merci!

Vielen Dank!

Questions

"Les cybermenaces à l'horizon 2020"