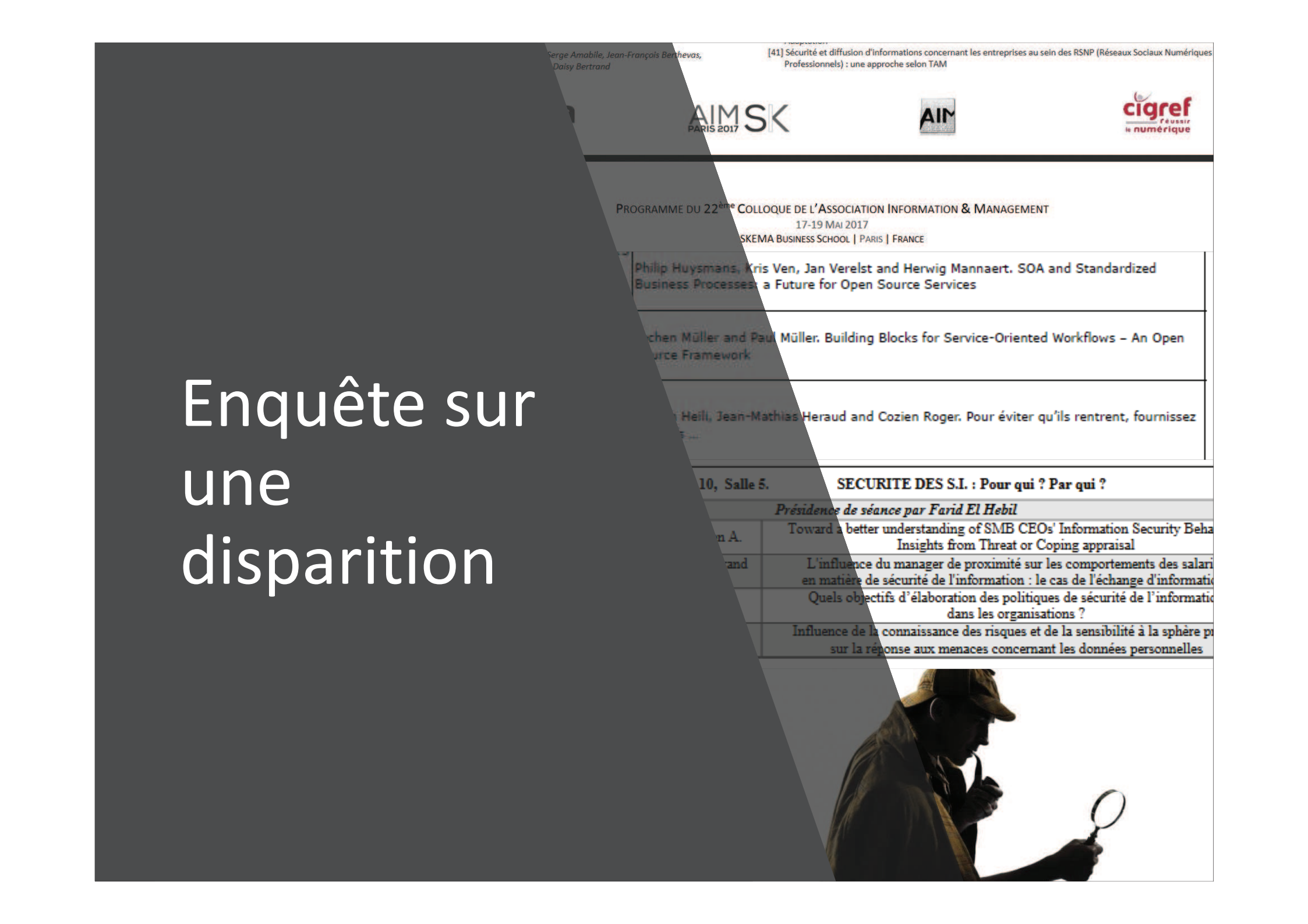
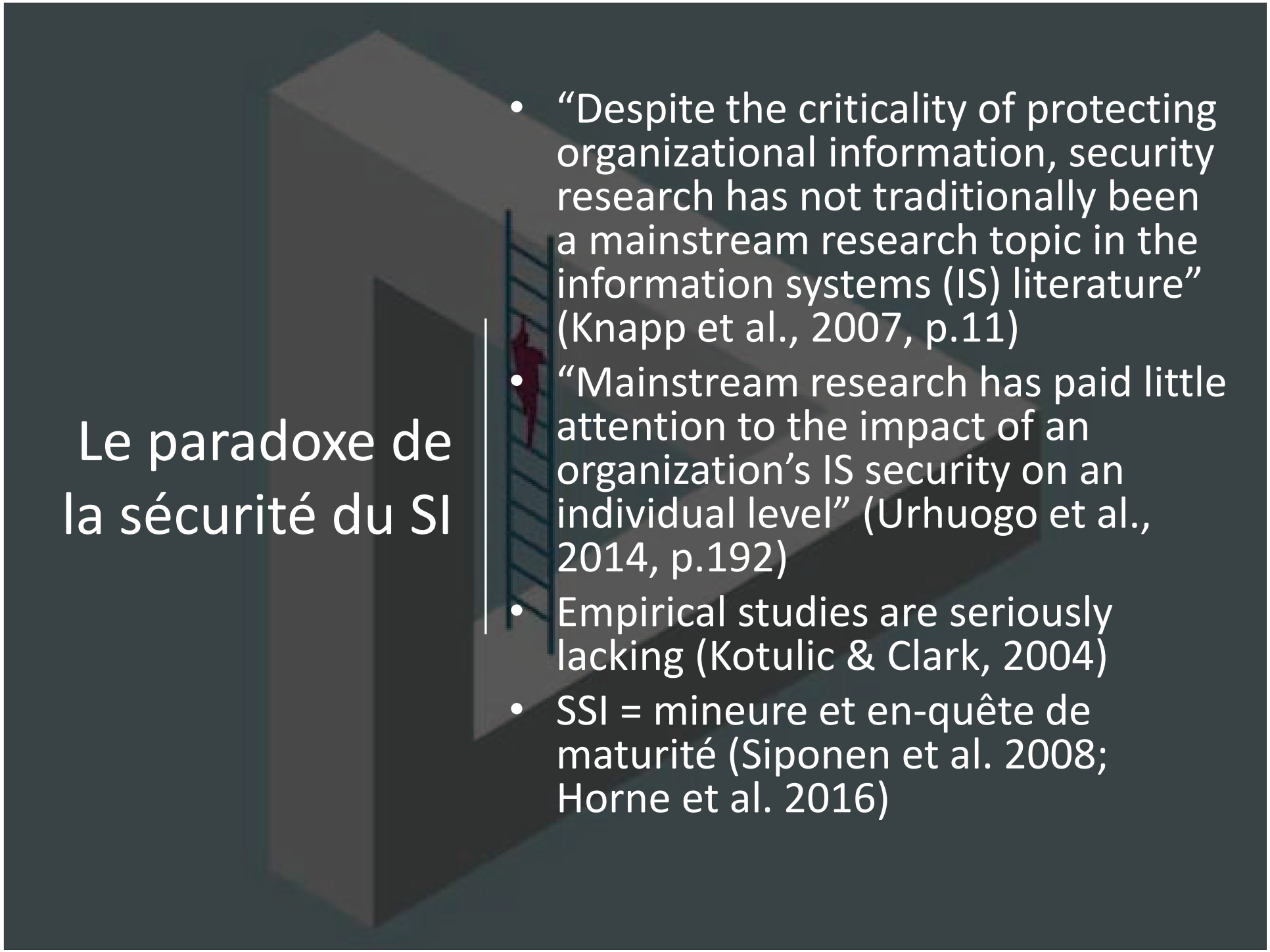
De la théorie à l'échec ? Complexité de la sécurité des SI

Jean-Loup Richet

Enquête sur une disparition





Le paradoxe de la sécurité du SI

- “Despite the criticality of protecting organizational information, security research has not traditionally been a mainstream research topic in the information systems (IS) literature” (Knapp et al., 2007, p.11)
- “Mainstream research has paid little attention to the impact of an organization’s IS security on an individual level” (Urhuogo et al., 2014, p.192)
- Empirical studies are seriously lacking (Kotulic & Clark, 2004)
- SSI = mineure et en-quête de maturité (Siponen et al. 2008; Horne et al. 2016)

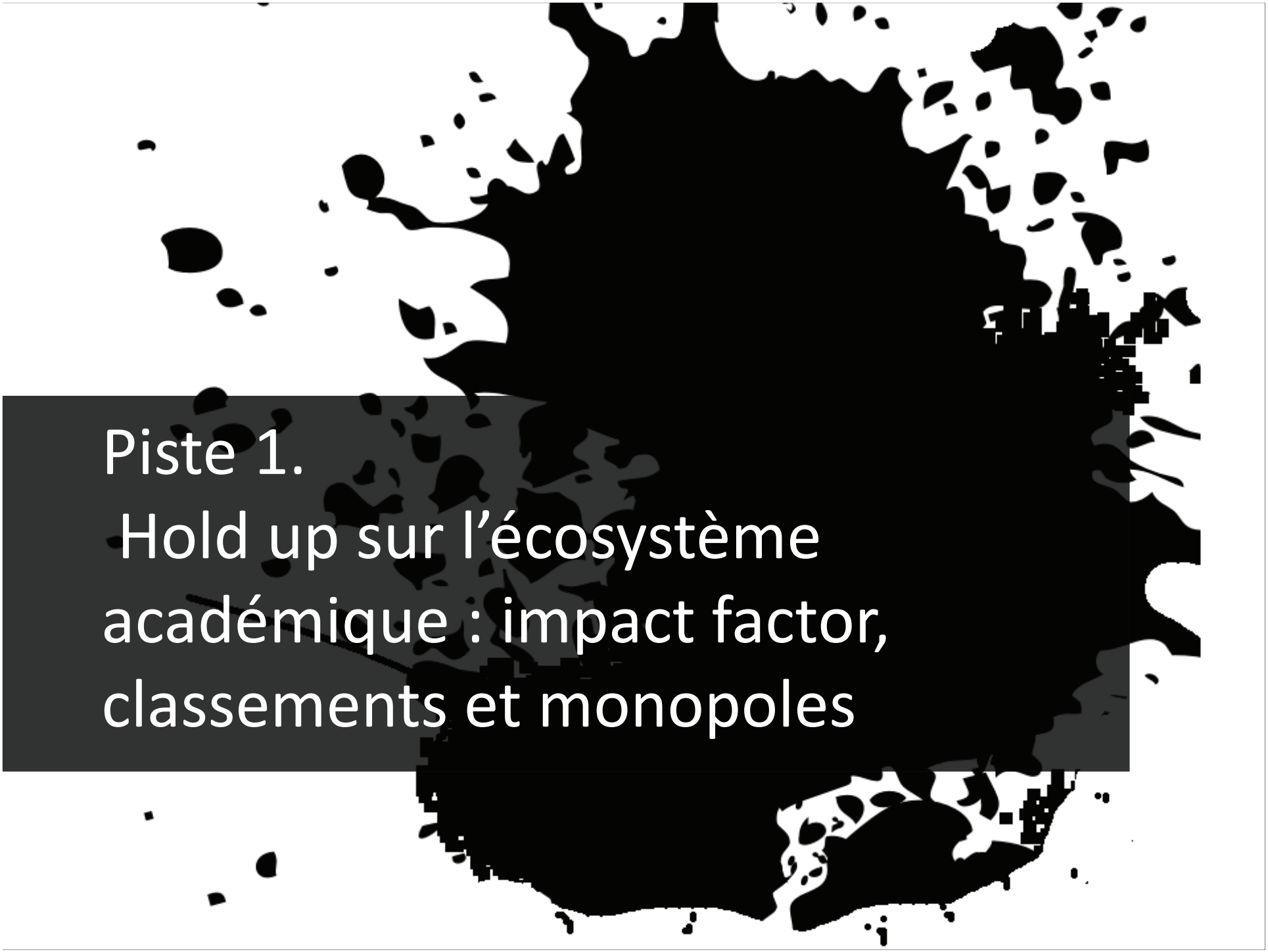
Programme de l'enquête

Piste 1. Hold up sur l'écosystème académique : impact factor, classements et monopoles

Piste 2. Recel de peer reviews : séparer le bon grain de l'ivraie

Piste 3. Blanchiment de littérature : quels concepts en Sécurité des SI ?

Conclusion. Non assistance à recherche en danger?


Piste 1.
Hold up sur l’écosystème académique : impact factor, classements et monopoles

Pourquoi publier dans les revues académiques ?

- Dès les débuts (1665) : revendication de paternité, diffusion des résultats, reconnaissance personnelle
- Evolution récente (science citation index, 1963) : explosion du nombre de papiers publiés (+50% entre 1990 et 2009; 1,4M par an)
- Importance décroissante de la diffusion des résultats (internet, accès libre)
- importance croissante de la reconnaissance personnelle (facteur d'impact)
- Evaluation de la production scientifique et de son impact

"I haven't been in any academic journals but I do get my Tweets re-Tweeted a lot."

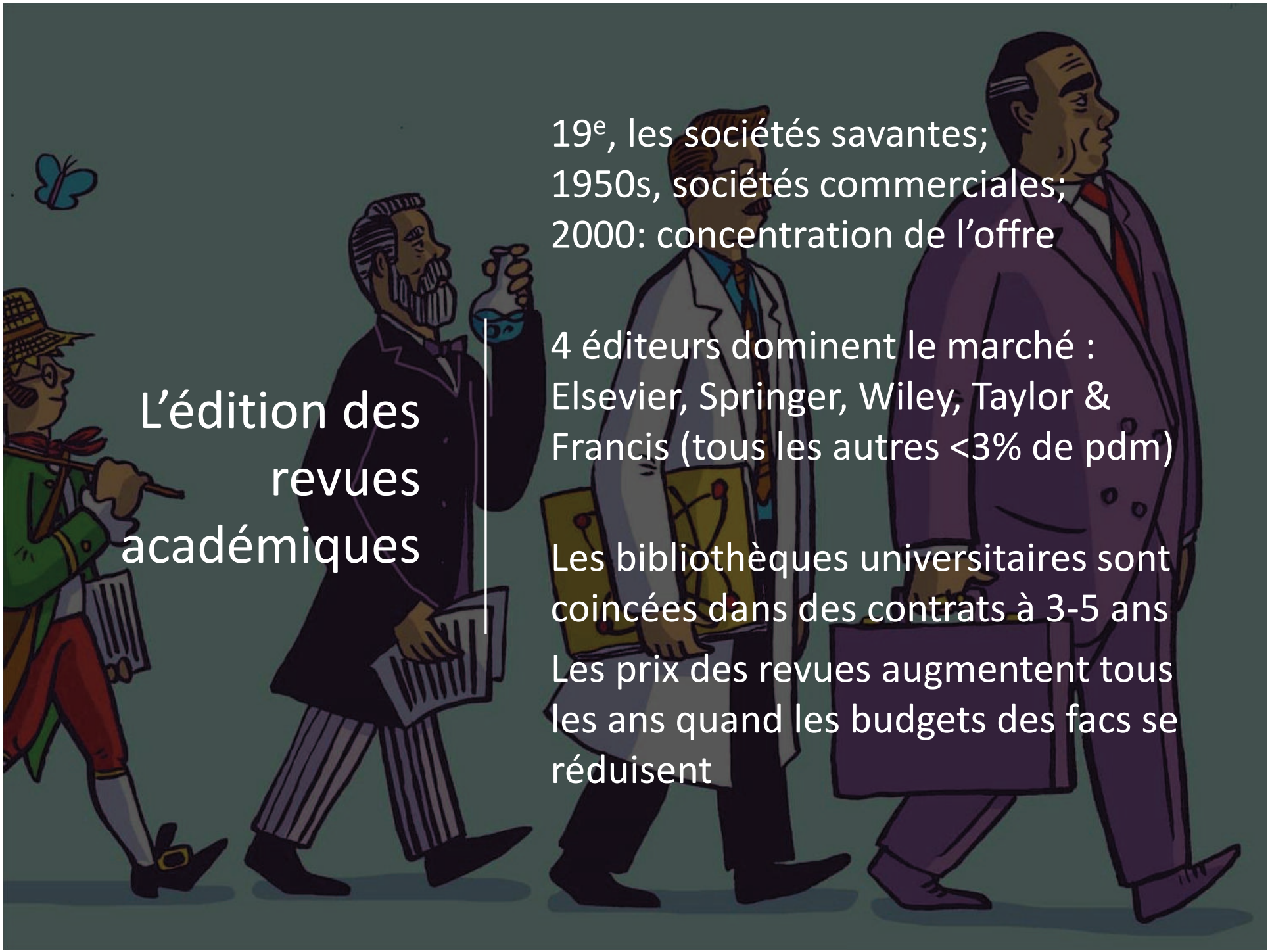
- KPI quantitatifs
- Mesurer par le tx de publications
- Evaluation : des chercheurs, des publications, des articles, des départements, etc
- Impact Factor & King makers

Gobert, 2008. Les dessous de la publication scientifique, IRD

Le facteur d'impact

Qualité scientifique ? marque de prestige ?
Un indice à manipuler avec prudence (pas universel)

Qualifie une revue (vs article). 50% des citations pour 15% des articles (90% / 50%)


L’édition des revues académiques
19e, les sociétés savantes;
1950s, sociétés commerciales;
2000: concentration de l’offre
4 éditeurs dominent le marché : Elsevier, Springer, Wiley, Taylor & Francis (tous les autres <3% de pdm)
Les bibliothèques universitaires sont coincées dans des contrats à 3-5 ans
Les prix des revues augmentent tous les ans quand les budgets des facs se réduisent

Conséquences pour l'écosystème académique… En quoi cela concerne la SSI ?

La course à l'IF : les petites revues spécialisées sont abandonnées par les éditeurs (vision business)

Concentration et 'big deals', le cercle vicieux. Inégalité croissante dans l'accès à l'information : s'il faut choisir, on ne s'abonne qu'aux plus grosses revues

Perte de contrôle de la communauté scientifique : influence des éditeurs sur les sujets (trends pour ventes et IF), génère alignement des soumissions. Young, 2008: *this system hold back scientific progress*

Piste 2.
Recel de peer reviews : séparer le bon grain de l’ivraie

Pourquoi faire des revues par les pairs ?

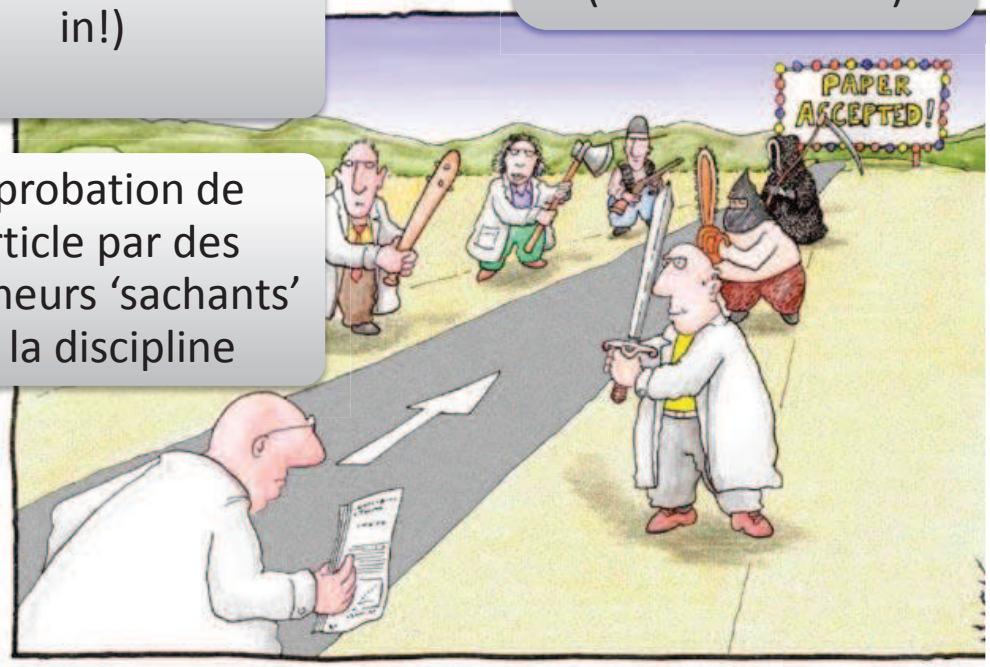
Filtrer

Capacité limitée de publication, plus de papiers soumis que publiés

Eliminer les papiers « mauvais », pseudo scientifiques, dommageables pour l'intérêt de la science (i.e. tobacco cie)

Aura de qualité (best in!)

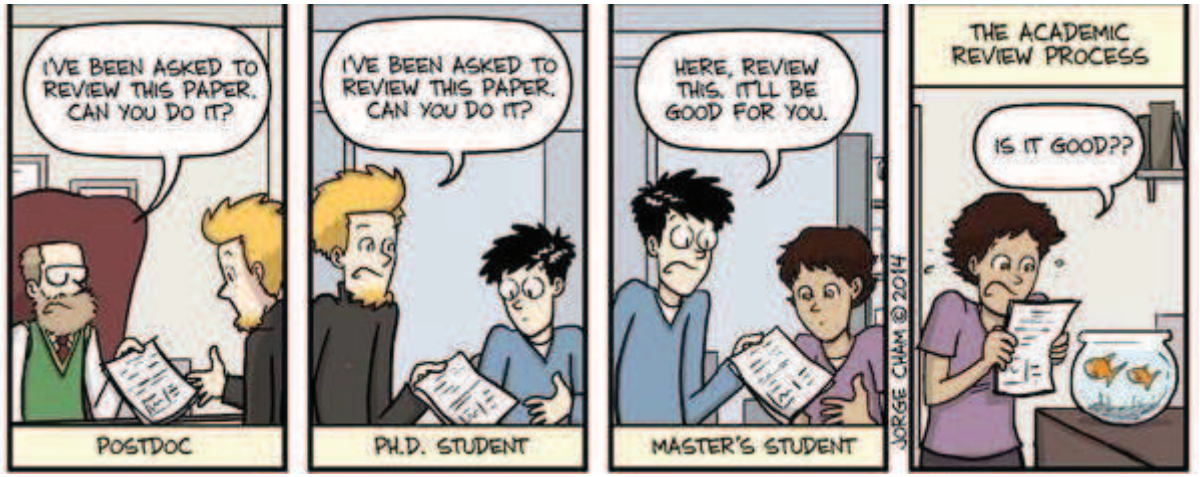
Approbation de l'article par des chercheurs 'sachants' de la discipline



Most scientists regarded the new streamlined peer-review process as 'quite an improvement.'

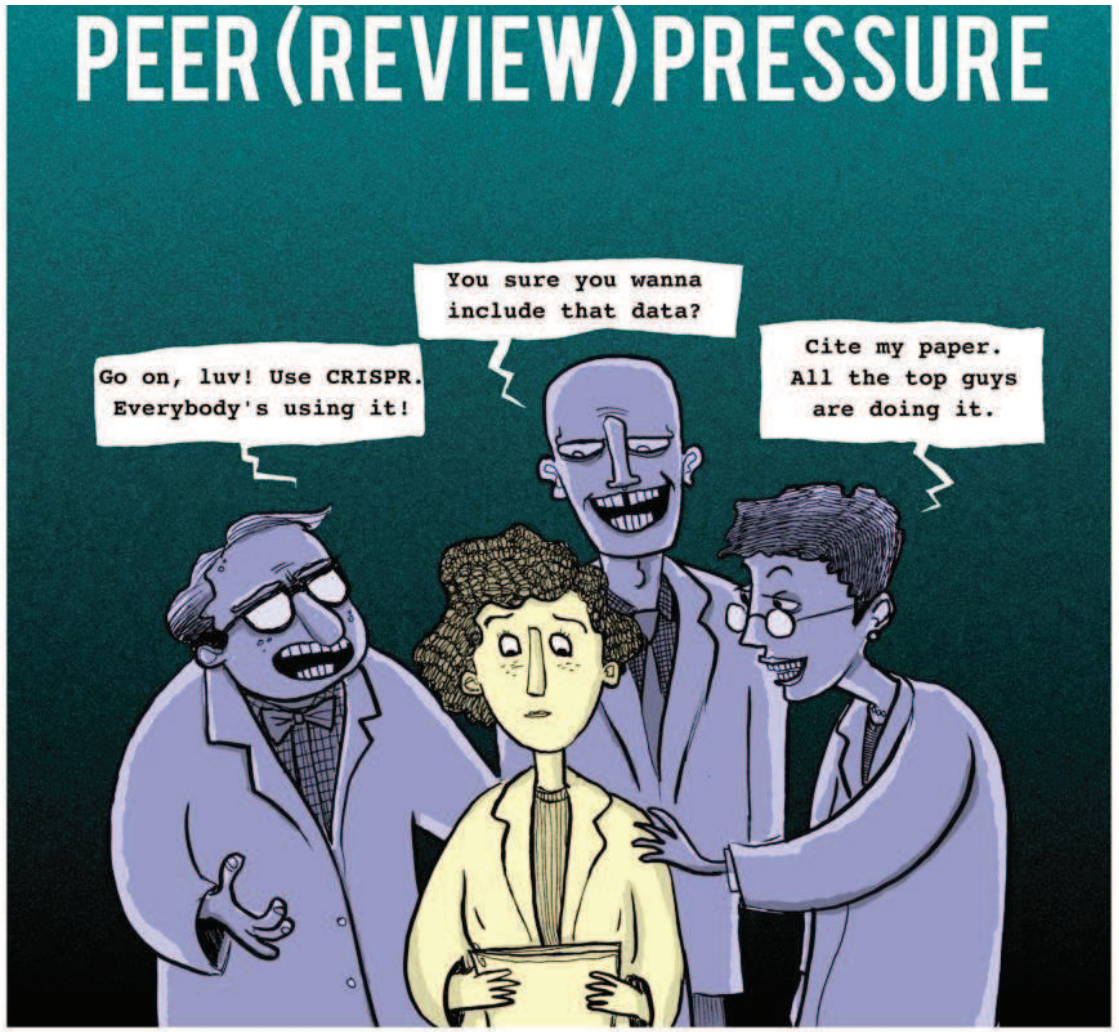
Le problème ?

- Des revues par les pairs qui valident la forme mais pas le fond ?
  - Jan Hendrik Schon (Bell Labs) 15 papiers publiés dans Science et Nature (1998-2001) qui furent révélés frauduleux
  - Igor and Grichka Bogdanov 1999 & 2002 deux papiers en physique théorique, largement critiqués pour leurs riche usage de jargons et de mots valises
  - L'affaire Sokal
- Les papiers en dehors des clous
  - Krebs & Johnson, 1937, rôle de l'acide citrique sur le métabolisme, rejeté par Nature comme 'non important', prix nobel 1953 (cycle Krebs)
  - Black & Scholes 1973 , modèle math de marché et d'éval d'option, rejeté par les meilleures revues, Nobel 1997



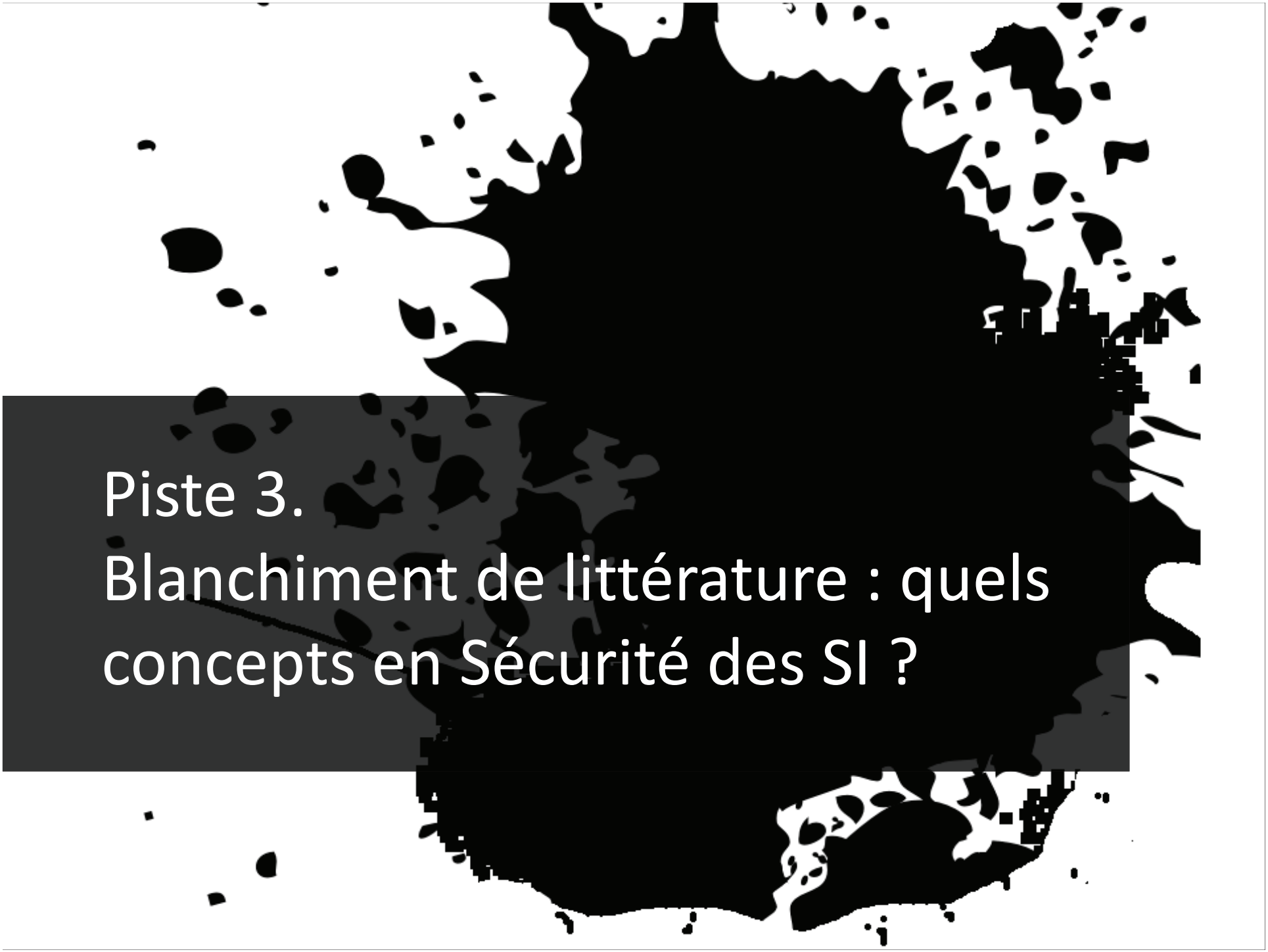
Une revue sous influences

- Vision erronée (ancienne ?) des apports de la recherche pour la discipline – *ce sujet n'est pas pertinent*
- Ignorance (volontaire ?) des autres parties prenantes (lecteur, praticien, etc)
- Complexification du message – *il faudrait ajouter un lien avec la théorie de zzz, parler de xxx et de yyy*

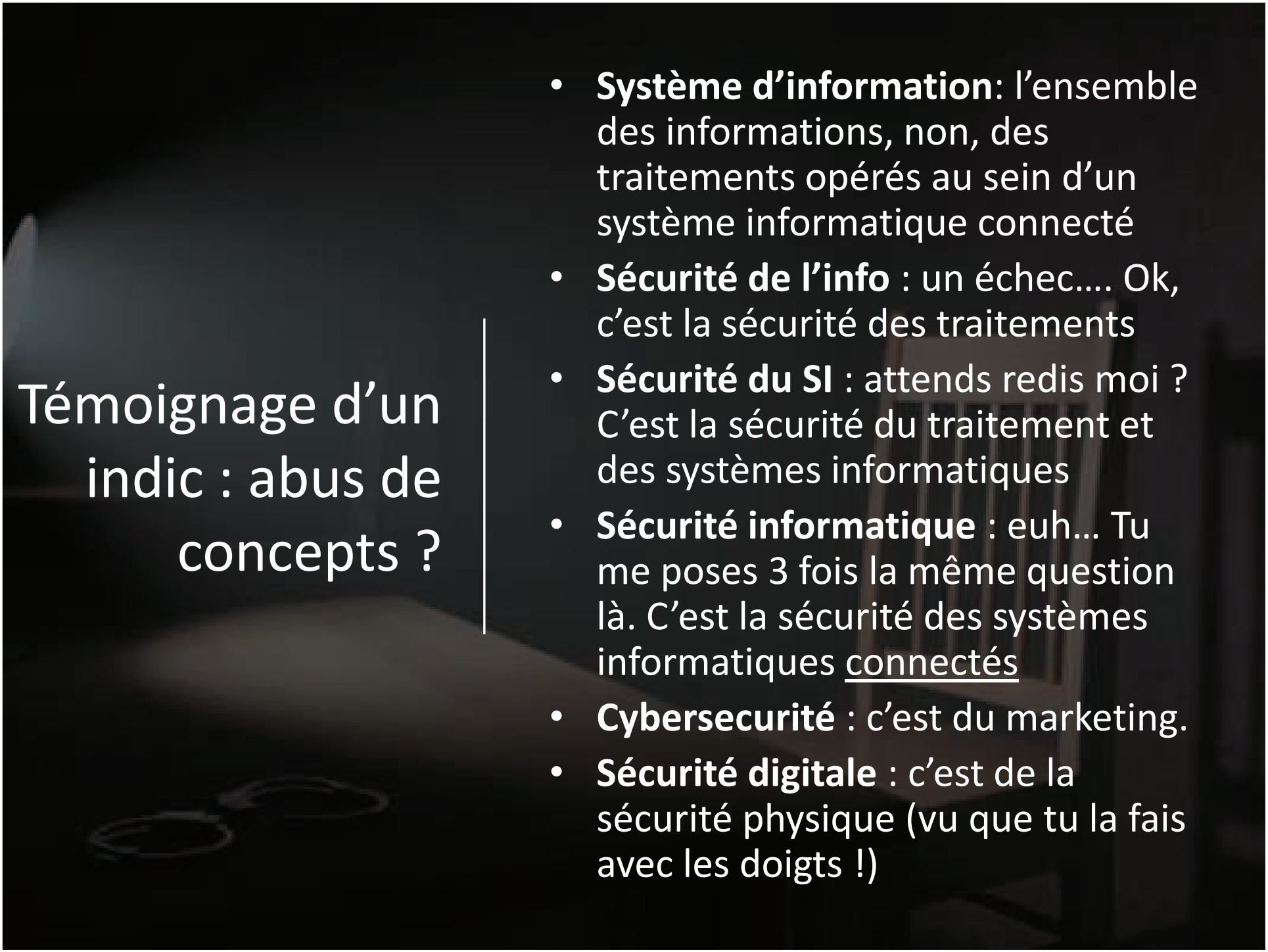


Wrap up des pistes 1 et 2 : la tyrannie des indicateurs scientométriques

- Conséquences pour les auteurs : publier toujours plus
  - publish or perish, rôle croissant de la revue comme "label" de prestige
  - Stratégies et tactiques (mainstream et revue classées, autocite, etc)
  - Décalage croissant entre l'écriture et la lecture de la science
- Conséquences pour les organismes : politiques scientifique et documentaires
  - Confusion entre excellence et élitisme (favoriser la revue classée prestigieuse sur la publication spécialisée de qualité)
  - Interprétation abusive du facteur d'impact et pilotage "au compteur"
  - Politiques d'abonnement des bibliothèques et sélection par l'argent (pays/organismes)
- Conséquences pour les éditeurs : la "course au facteur d'impact"
  - Création d'un marché générateur de profits, légitimité des "core journals" renforcée
  - Stratégies éditoriales (fuite du risque et suivi de tendances)
  - Encouragement voire pression à l'auto-citation des revues, menaces sur le système de peer-review (grilles d'évaluations fournies)



Piste 3.
Blanchiment de littérature : quels concepts en Sécurité des SI ?



Témoignage d'un indic : abus de concepts ?

- **Système d'information**: l'ensemble des informations, non, des traitements opérés au sein d'un système informatique connecté
- **Sécurité de l'info** : un échec…. Ok, c'est la sécurité des traitements
- **Sécurité du SI** : attends redis moi ? C'est la sécurité du traitement et des systèmes informatiques
- **Sécurité informatique** : euh… Tu me poses 3 fois la même question là. C'est la sécurité des systèmes informatiques connectés
- **Cybersecurité** : c'est du marketing.
- **Sécurité digitale** : c'est de la sécurité physique (vu que tu la fais avec les doigts !)

Dans les référentiels ?

Sécurité de l'information: ISO/IEC 27000:2016 (2.33): Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information

Sécurité du SI/numérique:

ANSSI 09/07/2009: GISSIP — Guide d'Intégration de la Sécurité des Systèmes d'Information dans les Projets

VS ANSSI 26/07/2017: Intégrer la sécurité numérique dans une démarche Agile

Cybersécurité: idem que sécurité de l'information, d'après la reco de l'ITU X.1205 (18/04/08)

Dans la presse et auprès du grand public ?

IT security *can probably be used interchangeably with cybersecurity, computer security and information security if it pertains to business* (Crawley, 2017 (Tripwire))

Cybersécurité : *measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack* (Dictionnaire Merriam-Webster)

Un flou pourtant bien perçu dans le monde académique

"La **cybersécurité** c'est comme la météo. Tout le monde en parle." (Shoemaker, Davidson & Conklin, 2017, P.12)

Dans la littérature académique, on mélange fréquemment sécurité de l'information et cybersécurité (Von Solms &Van Niekerk, 2013).

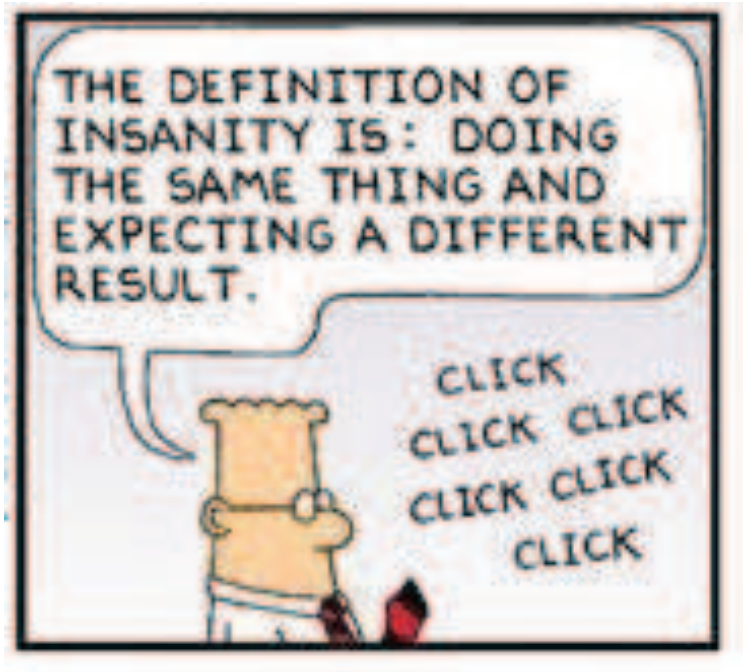
"le concept [de **Sécurité du SI**] est imparfaitement compris […] le SI est déjà un terme chapeau […] il y a de multiples définitions de sécurité informatique, sécurité de l'info et sécurité du SI mais on en revient toujours au CIA" (Horne, Ahmad & Maynard, 2016, p.1-4)

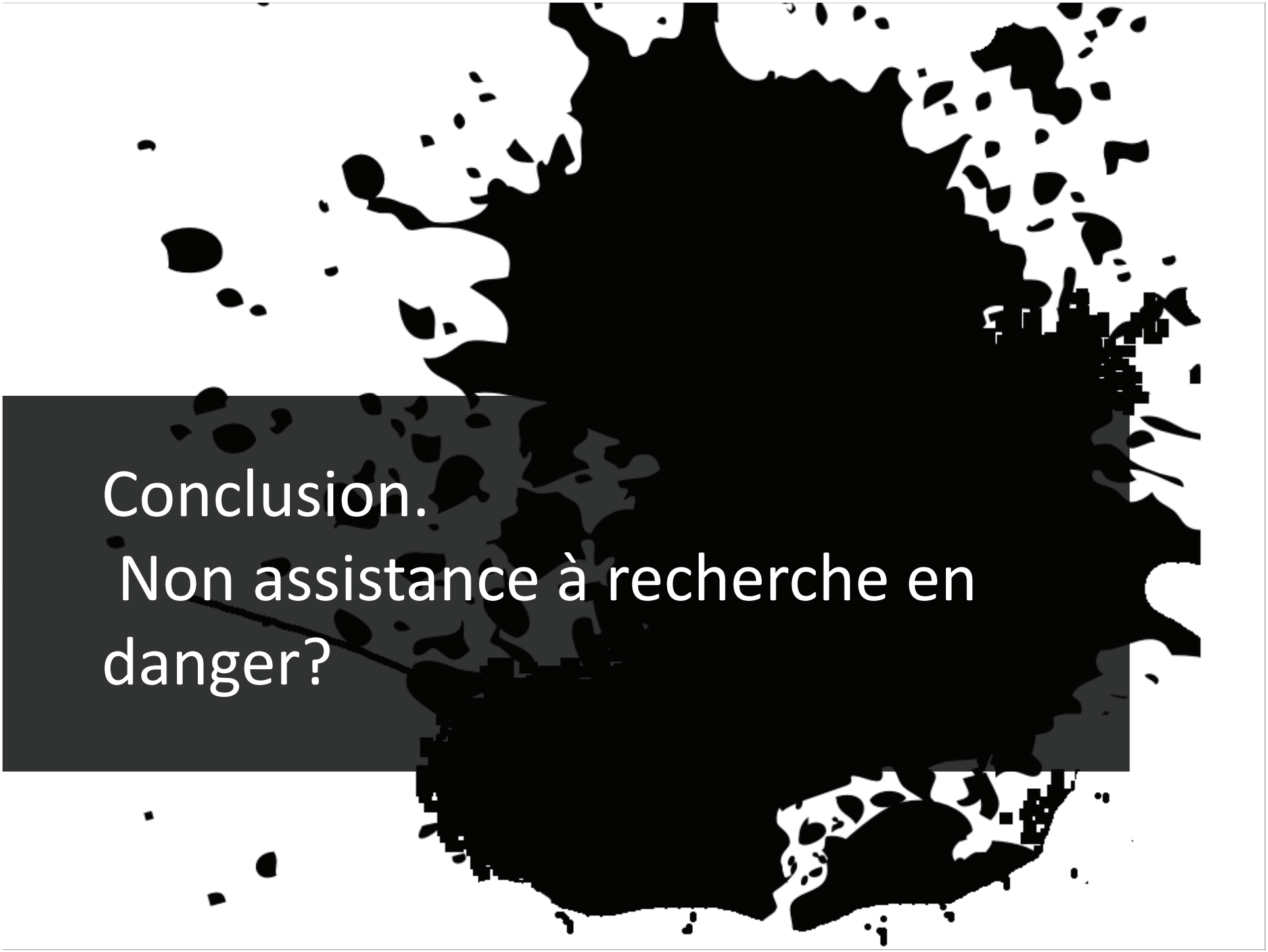
C'est la sécurité du système composé des hommes et du système informatique processant ou interpétant l'information (Horne, Ahmad & Maynard, 2016)

Cybersecu et SSI?

- Cybersécurité : un buzzword pour les experts, un synonyme de sécurité informatique selon le dictionnaire, un synonyme de sécurité de l'information pour les référentiels

- Sécurité du SI : … traitement, numérique, cycle de vie projet.
  Aspect orga ou synonyme de sécu informatique suivant les experts…




Conclusion.
Non assistance à recherche en danger?

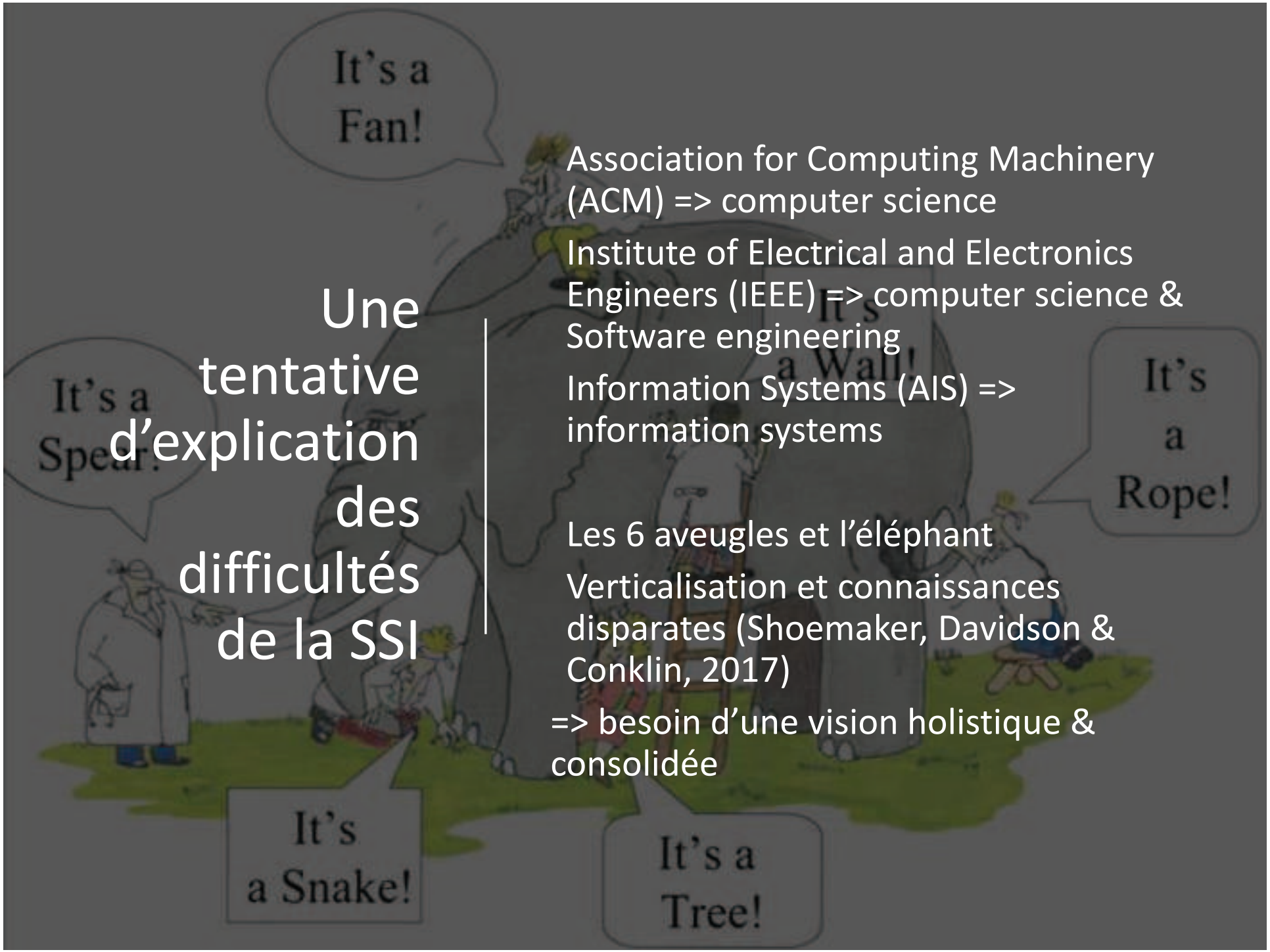
Les sables mouvants de la SSI

Sécurité des systèmes d'information : faible conceptualisation en SI (méthodo, taxonomie, model, plutôt apportés par les Computer Sciences). Flou sur les définitions, pour les chercheurs comme praticiens

Une discipline fondée sur la technique, qui évolue vers la socio-technique

Cyber sécurité : concept en mutation ? (cyberguerre, géopolitique, cyberdéfense, etc) VS usage courant

La SSI dans la littérature académique française : à explorer, mais étude préliminaire peu inspirante en SI (15 papiers sur 881!) : manque de maturité et de reconnaissance… S'il n'y a pas de perspective dans la recherche francophone, il y a (beaucoup) plus d'espoirs à l'international



Une tentative d'explication des difficultés de la SSI

Association for Computing Machinery (ACM) => computer science

Institute of Electrical and Electronics Engineers (IEEE) => computer science & Software engineering

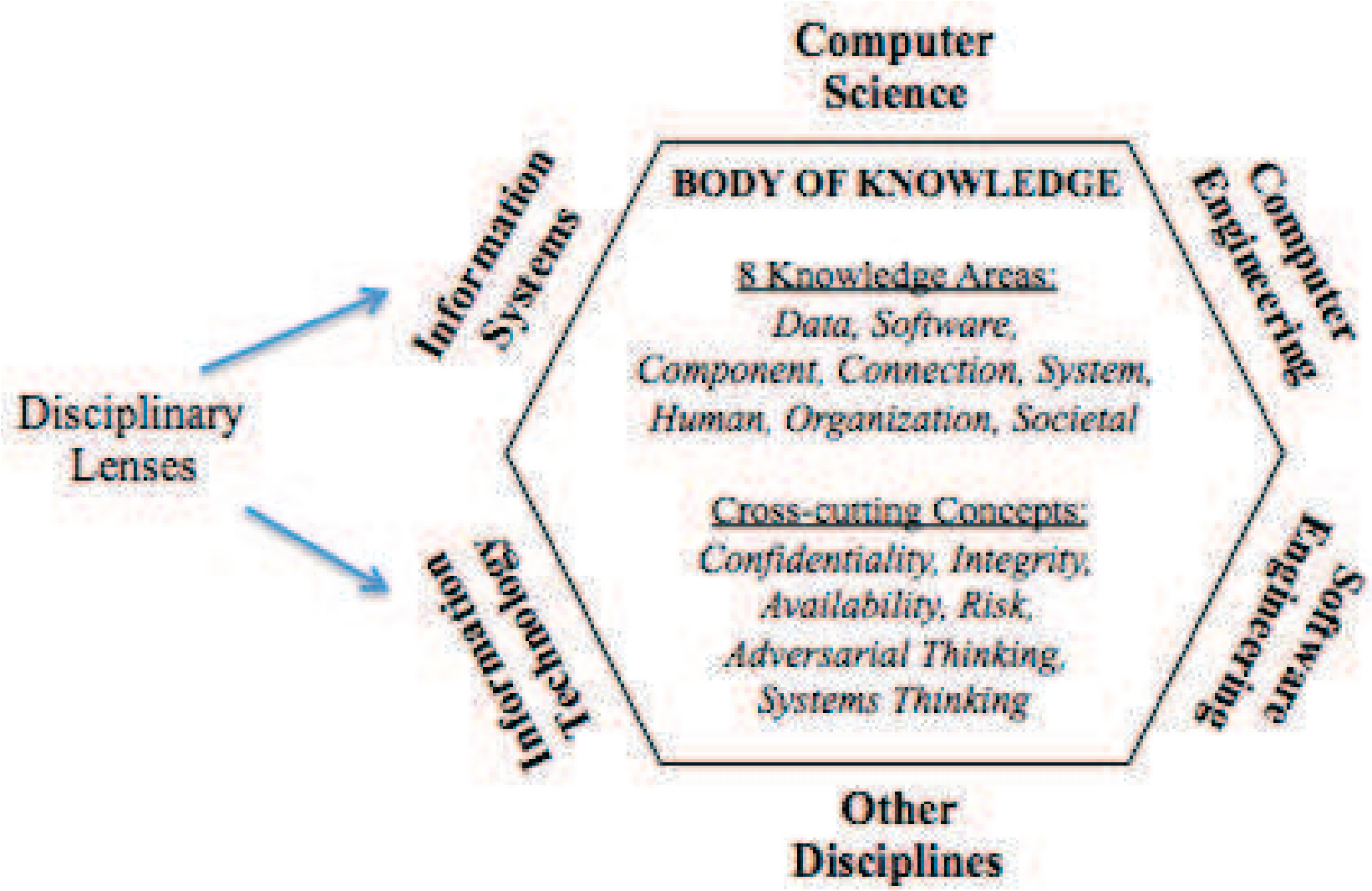
Information Systems (AIS) => information systems

Les 6 aveugles et l'éléphant

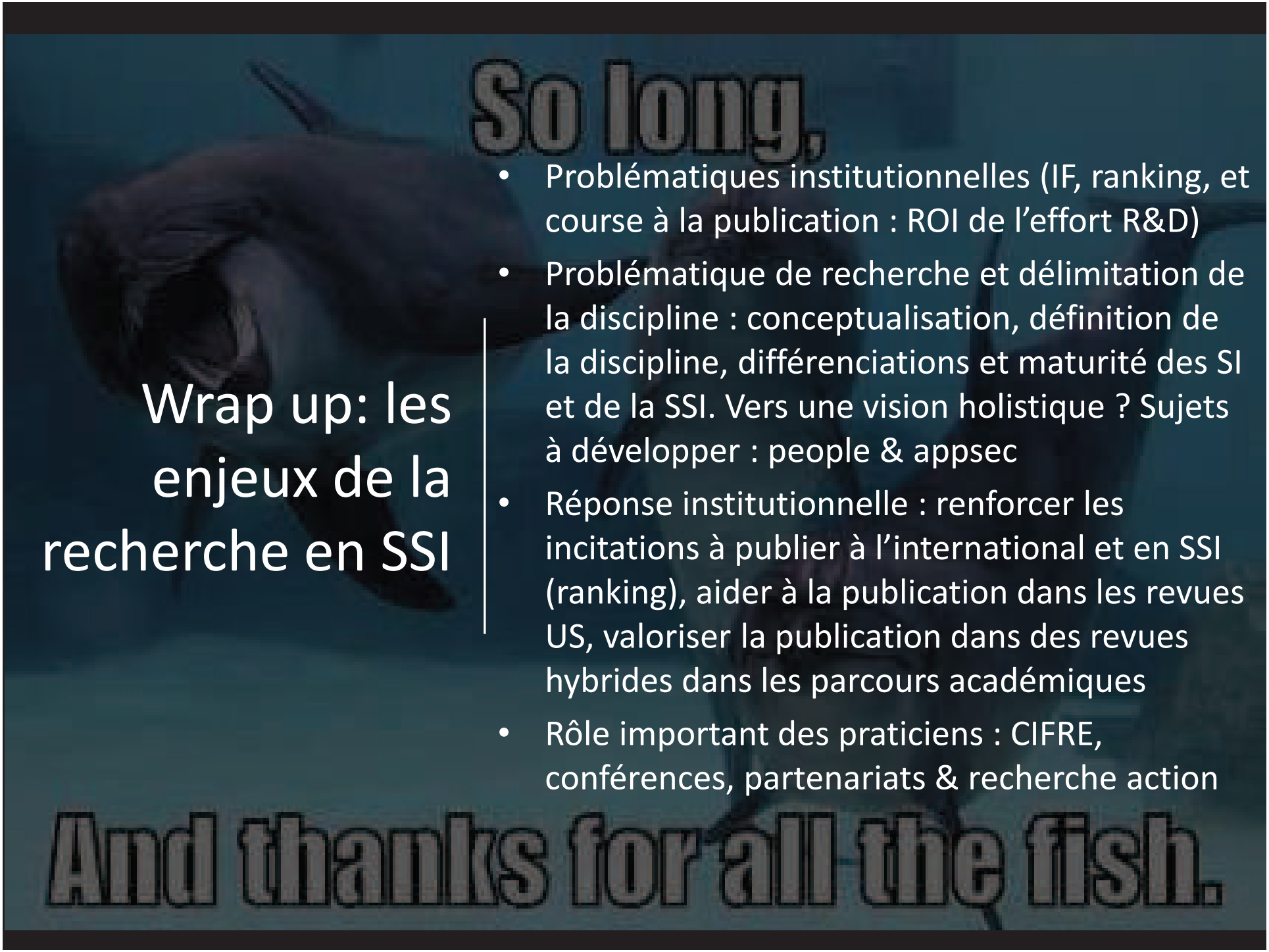
Verticalisation et connaissances disparates (Shoemaker, Davidson & Conklin, 2017)

=> besoin d'une vision holistique & consolidée

Vers une perspective holistique



(CSEC2017 JTF – IEEE CS, ACM, IFIP WG 11.8 et AIS)



Wrap up: les enjeux de la recherche en SSI

- Problématiques institutionnelles (IF, ranking, et course à la publication : ROI de l'effort R&D)
- Problématique de recherche et délimitation de la discipline : conceptualisation, définition de la discipline, différenciations et maturité des SI et de la SSI. Vers une vision holistique ? Sujets à développer : people & appsec
- Réponse institutionnelle : renforcer les incitations à publier à l'international et en SSI (ranking), aider à la publication dans les revues US, valoriser la publication dans des revues hybrides dans les parcours académiques
- Rôle important des praticiens : CIFRE, conférences, partenariats & recherche action