Penser la cybersécurité à l'heure de l'intelligence artificielle agentique

Solange Ghernaouti

Solange.ghernaouti@heptagone.ch

www.solange-ghernaouti.com

Directrice, Swiss Cybersecurity Advisory & Research Group

Présidente, Fondation SGH - Institut de recherche Cybermonde

Fondatrice - Associée Hepatgone Digital Risk Management & Security

SCARG
S. Ghernaouti

16.02.2026

FONDATION SGH
INSTITUT DE RECHERCHE CYBERMONDE

- Contexte
- Considérations à partir de différents points de vue
  - Des personnes
  - Des organisations
- Ce que fait l'IA agentique à la cybersécurité
- Perspectives

Plan

Illustrations

Dessins : Pecube

Photos : Pixabay.com

SCARG

S.Gharbaoui

Point de vue

Des personnes et des droits humains

SCARG
S.Chernaouti

« Tous les êtres humains naissent libres et égaux en dignité et en droits »

Déclaration universelle des droits de l'homme – 1948

Articles concernés

1, 2, 3, 4, 6, 7, 8, 12, 19,

20, 21, 23, 24, 28

SCARG

S.Gharnaouti

Protection des données

Ecosystème numérique

Modèles économiques

Smart cities

« Smart everything »

SCARG

S.Ghernaouti

IA

Facteurs aggravants

Omniprésence Permanence

Invisibilité

Physique Cyber

Récits

SCARG
S.Gharnaouti

Privacy & Protection des données

On se savait pas faire avant l'IA …

…On ne sait toujours pas

SCARG
S.Gharbaoui

Point de vue

Des organisations

SCARG
S.Chernaouti

Risques

Délégation

Responsabilité

Justification

Vérifiabilité

Traçabilité

SCARG

S.Gharsellaoui

Asymétrie du pouvoir de contrôler

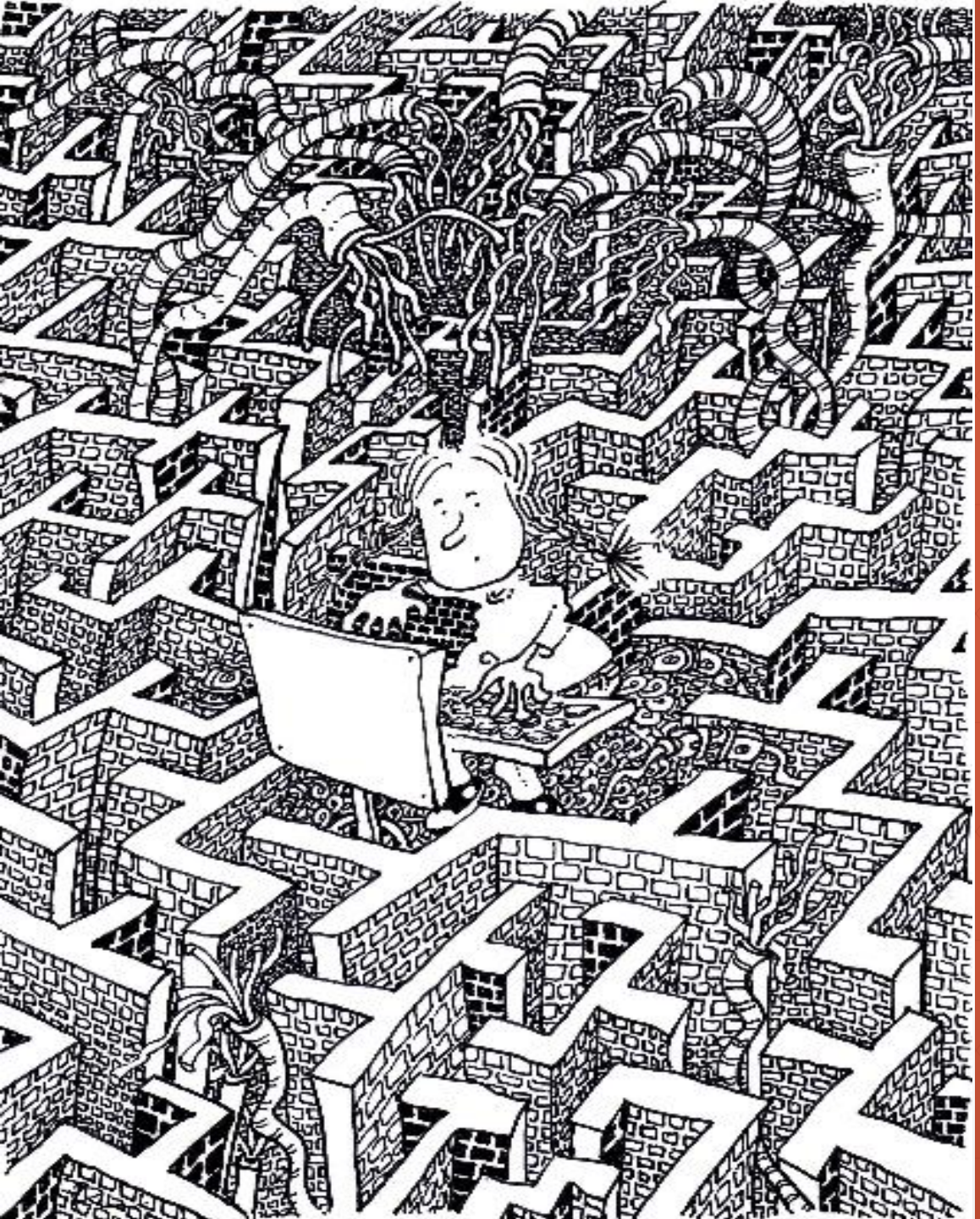
Confidentialité

Propriété intellectuelle

Savoir faire

Compétitivité

SCARG
S.Gherpescuti



IA « Une boite noire »

Obscurité

Données

Apprentissage

Mises à jour

SCARG

S.Gharsellaoui

IA agentique pourquoi faire?

Plus d'IA dans l'IA ?

Plus de complexité ?

Plus de dépendance ?

Plus de risques ?

- Design
- Architecture

SCARG

S.Ghernaouti

Cybersécurité

Qui fait ?

Qui paye ?

Qui est responsable?

Cyber Insécurité

Qui en supporte les conséquences?

SCARG
S.Gharnaouti

Point de vue

De la cybersécurité

Usages & Sécurité globale – Sécurité des agents

SCARG

S. Chennoufi

Choix
Managérial
Organisationnel
Technique
Procédural

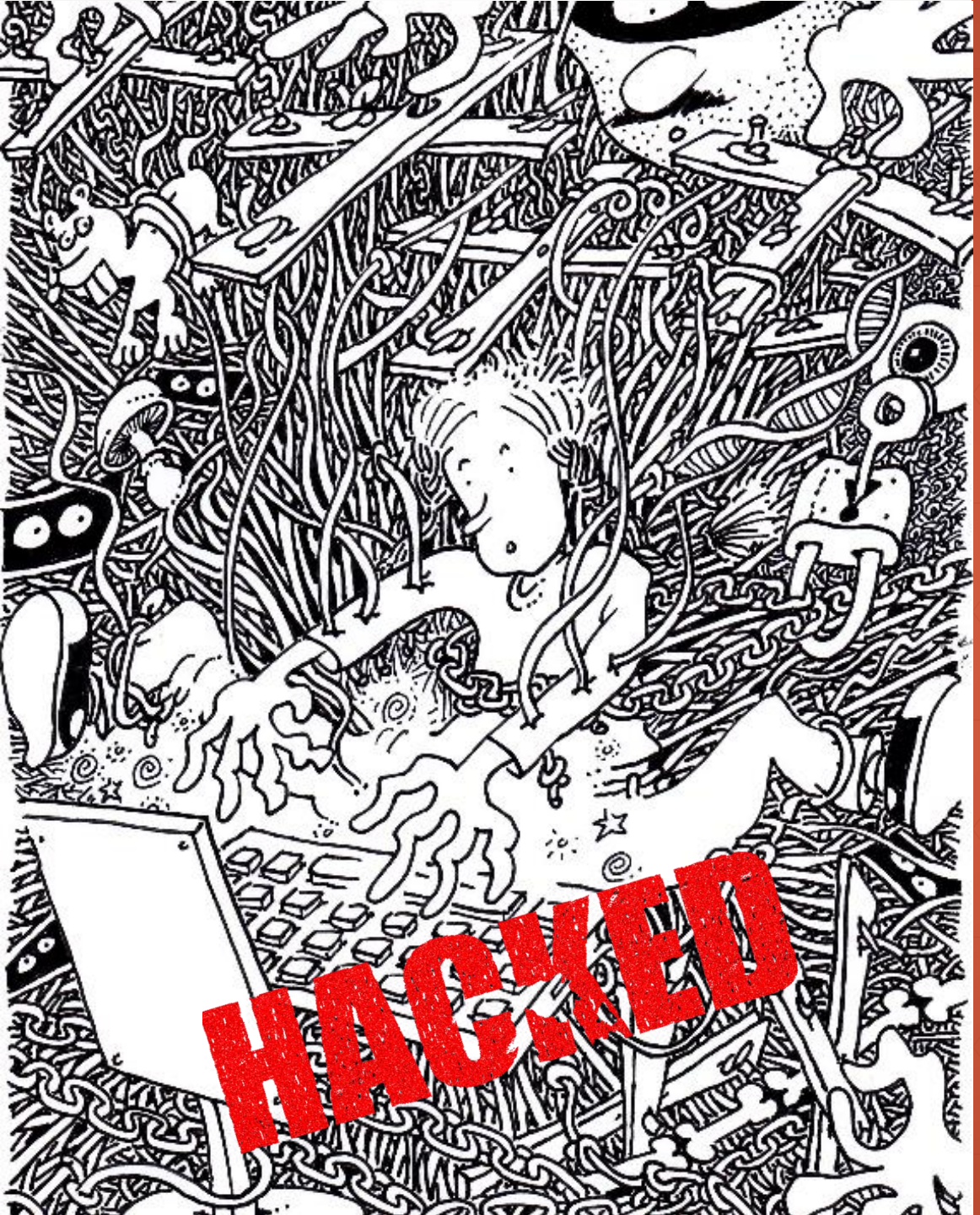
A quoi sert l'IA en cybersécurité?

Quels sont les apports de l'IA agentique

Quels degrés d'autonomie?

Quels degrés d'intégration?

SCARG
S.Ghernaouti



Cyberecurité des agents IA

Conception

Déploiement

Utilisation

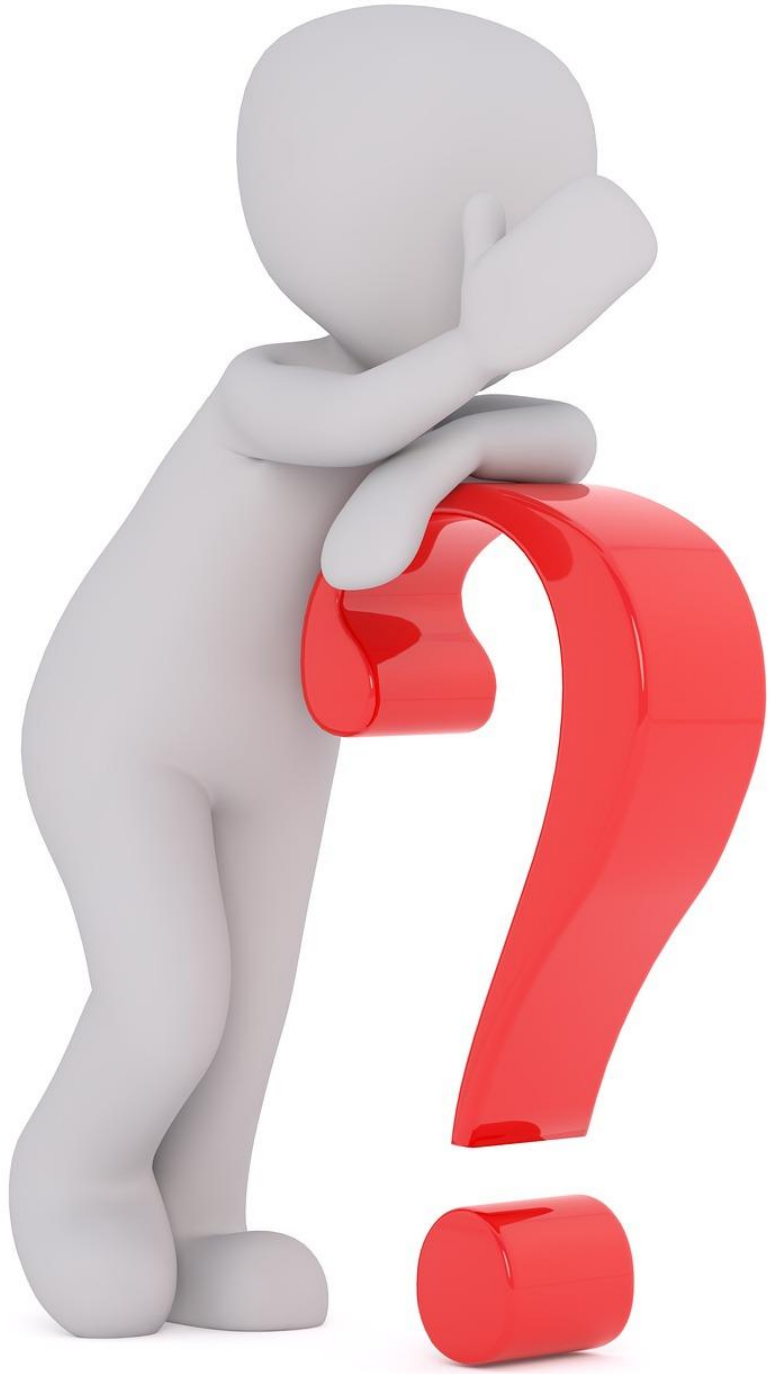
Cycle de vie

Cybercrime

L'IA: la nouvelle menace « Man In the Middle »?

SCARG

S.Chennaoui



Cybersécurité

Avant l'IA:

On ne savait pas bien faire

Avec l'IA:

On ne sait pas bien faire

L'IA un nouveau régime de:

Promesses

Croyances

SCARG
S.Gharbaoui

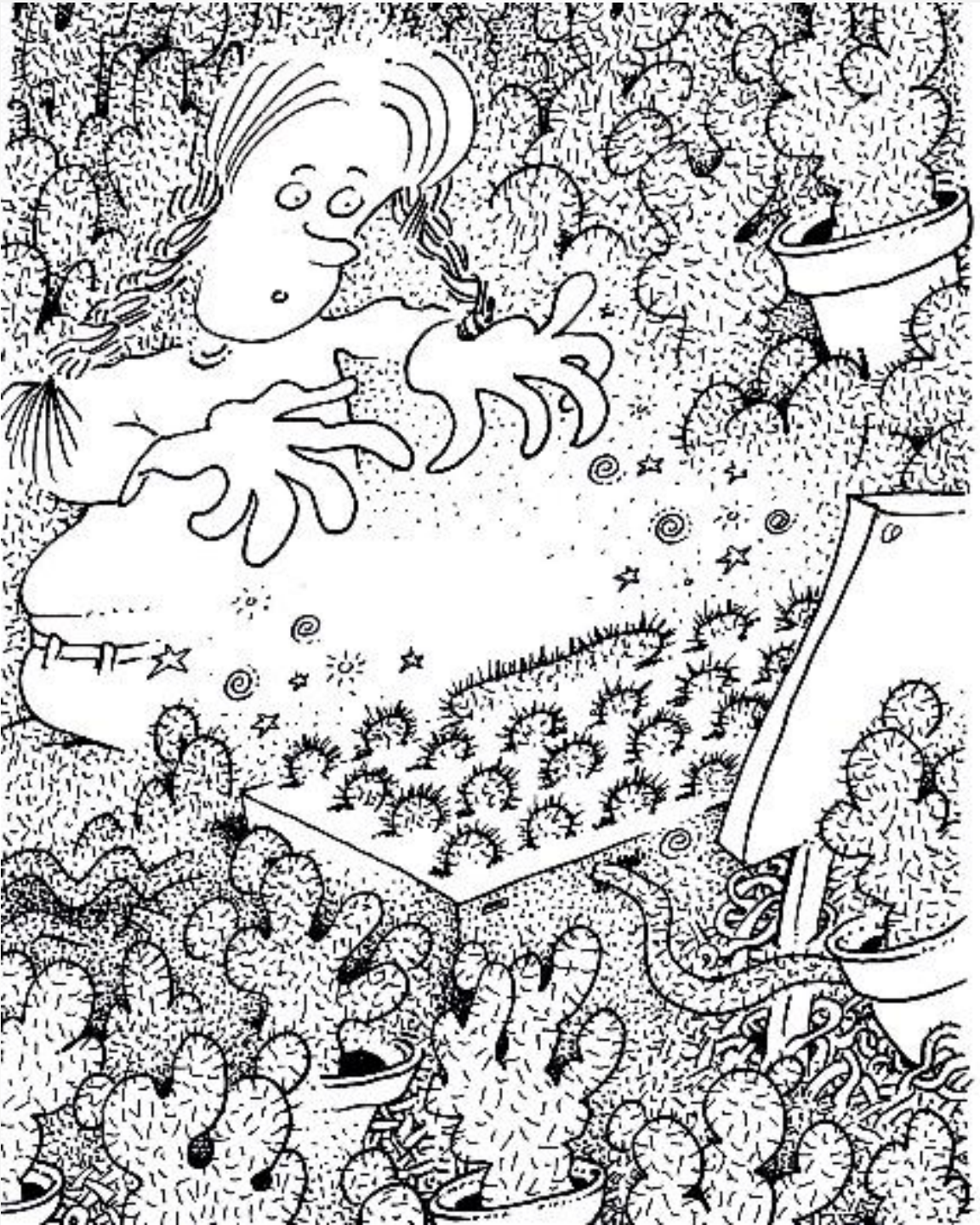
Problèmes de sécurité IA & IA agentique

conséquences structurelles

conception & usages

Dette technique

Dette sécuritaire



SCARG
S.Ghernaouti

Sécurité
Fiabilité
Confiance

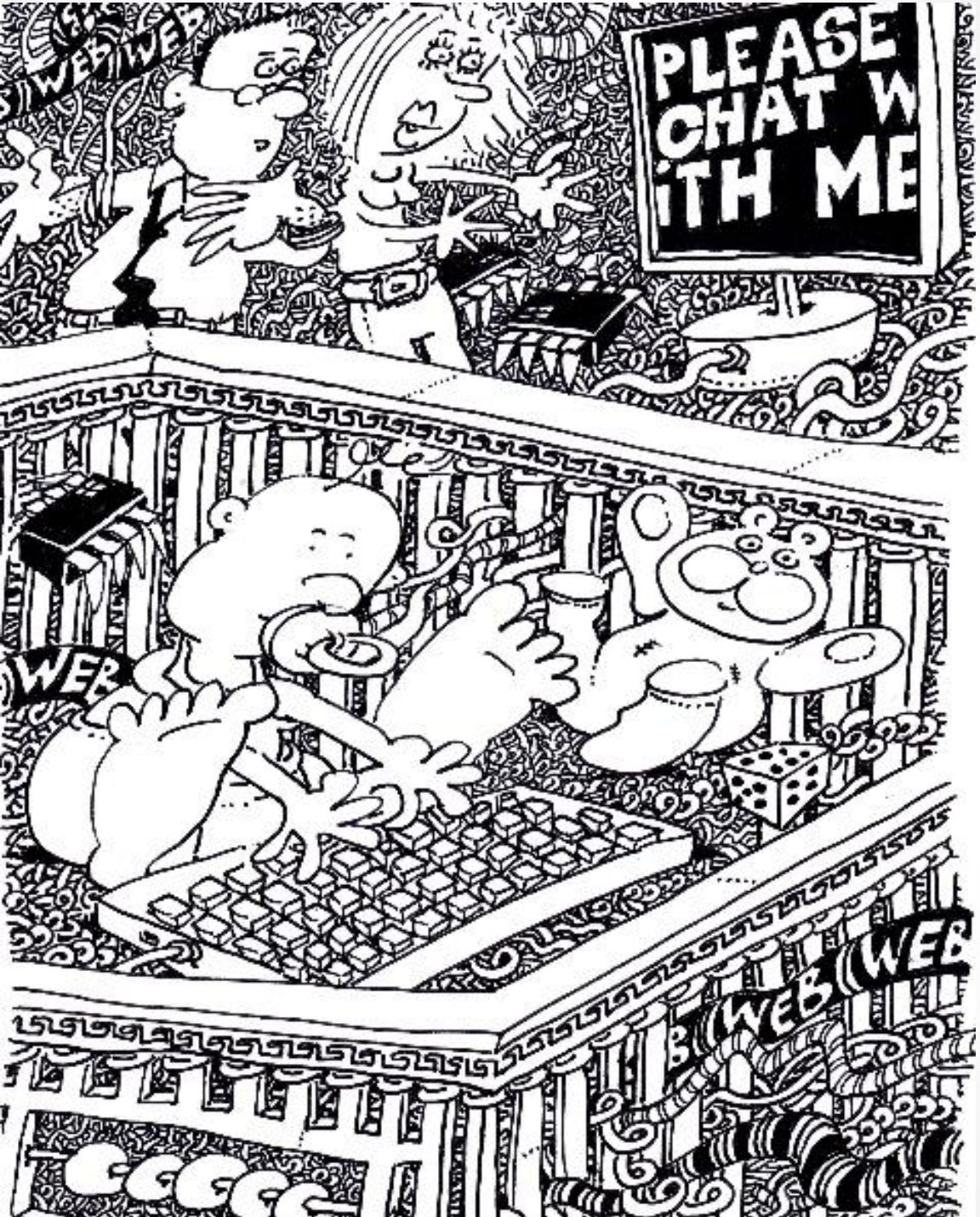
Développement - Intégration - Exploitation sécurisés ?

Défis:

- Rapidité

- Vérifiabilité

Interactions des agents / des compromissions ?



Problème original

Modélisation

Complexité

Conception

Mode de fonctionnement

SCARG

S.Ghernaouti

Injonctions contradictoires

Incompatibilités ontologiques

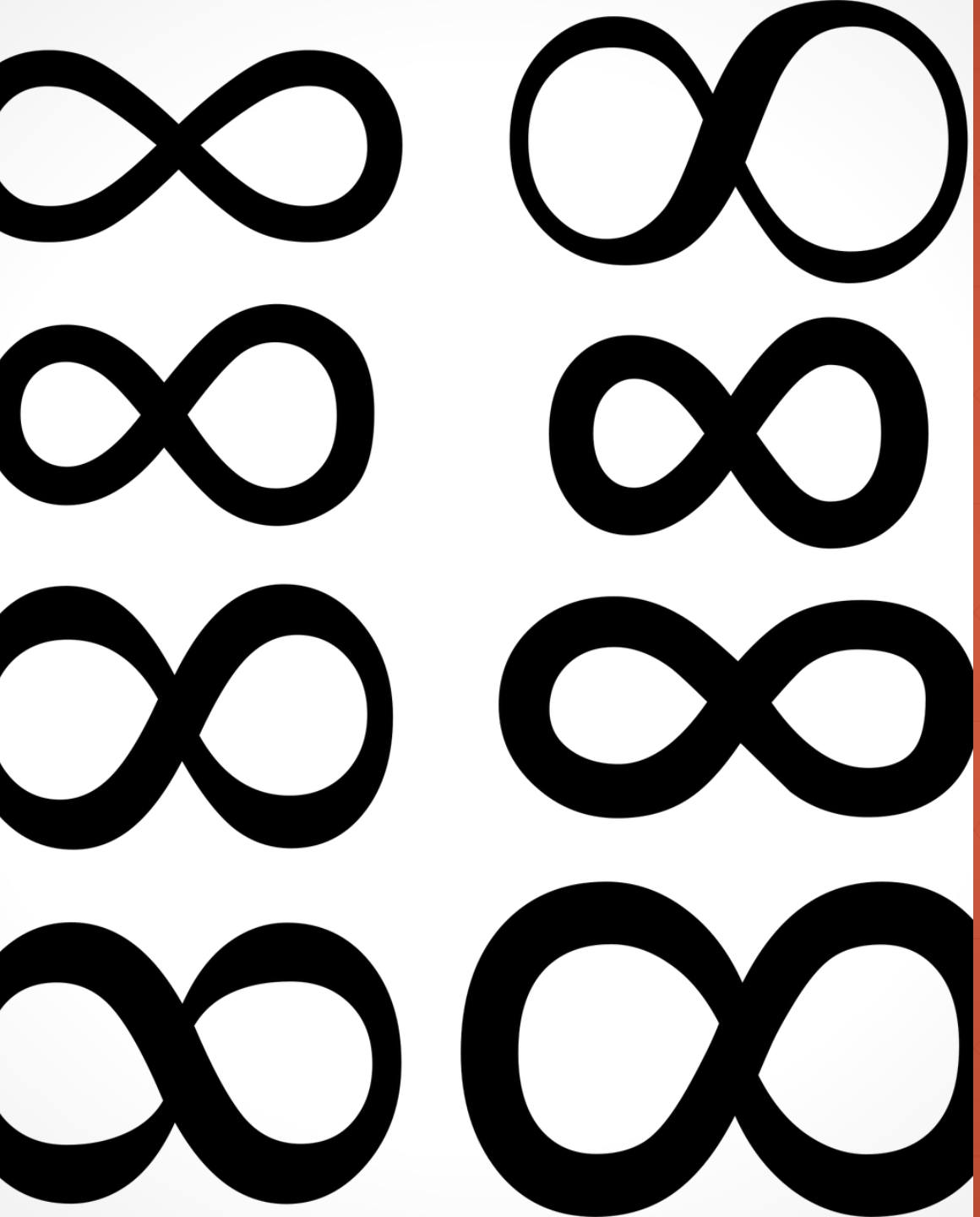
Rapide

Intelligent

Sécurisé

SCARG

S.Ghernaouti



SCARG
S.Chernaouti

La cybersécurité « *as usual* »

Management

IAA: un employé comme un autre?

Comment sécurisé la main d'oeuvre numérique?

Gestion des risques

Technique

0 trust

Gestion des identités, des contrôles d'accès, des …

Cloisonner, surveiller, contrôler,…

Point de vue

De la société & de la biodiversité

SCARG
S.Chernaouti

Innovation & Challenges

Finalités?

Construire plus de *data centers*

Augmenter l'extractivisme et la consommation numérique

Perspectives écologiques et environnementales

Illusions de souveraineté

…

SCARG
S.Gharnaouti

Asymétrie

Ressources

Capacités

Temps

Besoins

Pouvoir

...

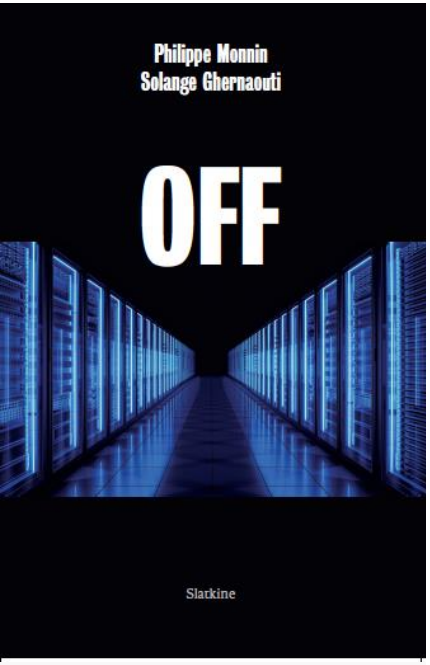
SCARG

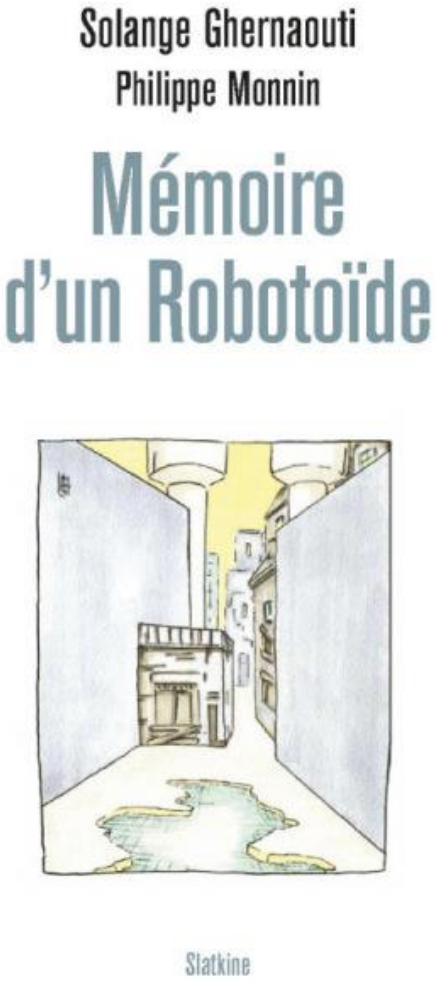
S.Gharnaouti

Perspectives

SCARG
S.Ghernaouti

Thank you for your attention





heptagone
digital risk management & security

Pecube