ARCSI
Association des Réservistes du Chiffre et de la Sécurité de l'Information

Université Paris Cité

Compte rendu du Lundi de la cybersécurité du 16 février 2026

# Penser la cybersécurité à l'heure de l'IA agentique

Organisé par Pr. Ahmed Mehaoua, Béatrice Laurent et Gérard Peliks
Rédigé par Rayan Al Mohaize, étudiant en Master 2 Cybersécurité

# Table des matières

# I Introduction

L'événement « Lundi de la Cybersécurité » est une série mensuelle de conférences en ligne créée et animée de manière indépendante par Gérard Peliks et Béatrice Laurent. Elle a pour vocation d'explorer chaque mois une thématique différente liée aux enjeux contemporains de la sécurité numérique et de la société.

## 1 Le thème de l'IA agentique et de la cybersécurité

Le Lundi de la cybersécurité du 16 février 2026 portait sur la place de la cybersécurité face aux IA agentiques : "Penser la cybersécurité à l'heure de l'IA agentique". Lors de ce webinaire, la réflexion s'est faite sur les différentes problématiques et difficultés auxquelles les professionnelles de la cybersécurité seront heurtées avec l'évolution de ces IA et comment parvenir à les surmonter.

## 2 Les intervenants

Pour animer ce Lundi de la cybersécurité, **Solange GHERNAOUTI**, professeure émérite à l'université de Lausanne et chercheure universitaire en cybersécurité et gestion des risques, nous a fait part de son expertise pour nous expliquer les enjeux de la cybersécurité dans le contexte de l'évolution des IA agentiques.

Par la suite, **Fabrice BRU**, président du CESIN, nous a présenté le Club des Experts de la Sécurité de l'Information et du Numérique, en nous exposant notamment les ambitions, les valeurs et les actions menées par le club ainsi que les principaux membres.

# II Penser la cybersécurité à l'heure de l'IA agentique (Par Solange GHERNAOUTI)

## 1 Point de vue des personnes et des droits humains

Pour commencer sa présentation, Solange GHERNAOUTI nous liste les articles de la Déclaration universelle des droits de l'homme sur lesquels l'IA pourrait avoir un impact. Par cela, nous comprenons que nous sommes aujourd'hui dans un contexte d'évolution de l'IA qui met à mal les droits fondamentaux.

En outre, des questions peuvent se poser dans le cadre de la protection des données : quels sont les droits des personnes à contrôler les données qui les concernent dans le contexte de l'utilisation de l'IA ? Et quelles sont les obligations des organisations dans la protection de ces données ? Ainsi, en essayant de répondre à ces questions, nous arrivons à la conclusion que nous ne pourrons pas répondre à l'entièreté des besoins de sécurité des données si notre modèle économique basé sur la rentabilité, que nous perpétuons avec l'IA et qui pose des problèmes à la propriété des données, n'est pas remis en question. Notre écosystème numérique est donc fait pour exploiter des données et non pas pour les protéger. Basé sur la croissance numérique et l'augmentation de la consommation, ce fonctionnement fait de nous, humains, un système d'information à part entière à partir duquel il faut extraire de

la donnée. Solange GHERNAOUTI nous parle ici de dépendance, voire de colonialisme numérique.

Plusieurs facteurs aggravants rendent l'IA puissante et dangereuse, notamment l'omniprésence, la permanence et l'invisibilité des techniques d'IA, ainsi que sa capacité à collecter massivement des données pour en faire des traitements qui échappent au consentement de l'utilisateur. Par ailleurs, l'IA est sujette à une guerre des récits, notamment entre les modèles américains et chinois, qui prend de plus en plus d'importance et qui nous fait rentrer dans un régime de croyance.

Enfin, Solange GHERNAOUTI nous explique que le droit ne suffit pas pour la protection des données car il ne résiste pas aux pressions des marchés et de l'innovation, ce qui expliquerait la réforme du RGPD qui est en cours, susceptible de réduire la protection des données pour suivre cette logique d'innovation.

D'après Solange GHERNAOUTI, la bataille de protection des données serait d'ores et déjà perdue.

## 2 Point de vue des organisations

On sait que les technologies d'IA que nous utilisons ne sont pas sécurisées nativement, donc il faut rajouter cette sécurité et donc alimenter le marché de la cybersécurité. Ainsi on peut se questionner sur la responsabilité du coût de cette sécurité : qui va payer ?

De plus, Solange GHERNAOUTI évoque le shadow IA comme un phénomène rendant difficile la vérifiabilité, l'auditabilité et la transparence, dues à la délégation et à l'externalisation de ces agents. Nous sommes ici dans une asymétrie du pouvoir, dans laquelle on se questionne sur qui doit contrôler et qui doit vérifier, alors que l'on sait qui porte la responsabilité financière. Ainsi Solange GHERNAOUTI affirme que les dirigeants sont des exécutants aux ordres de l'IA et sont confrontés à un pouvoir algorithmique qui leur est incontrôlable.

Par ailleurs, l'IA agentique représente un ensemble de boîtes noires qui interagissent entre elles et qui accèdent à des ressources externes, et cela pose encore une fois un problème de vérifiabilité et d'auditabilité. En effet, comme l'a évoqué Solange GHERNAOUTI, l'IA agentique "c'est plus d'IA dans l'IA", donc plus de complexité, plus de risque et plus de dépendance. La cybersécurité ne doit pas être le seul élément sur lequel nous devons nous appuyer pour réduire les risques et régler les problèmes de sécurité de l'IA, il faudrait agir directement sur les décisions managériales prises pour la conception de ces modèles.

## 3 Point de vue de la cybersécurité

Sur le point de vue de la cybersécurité, le problème ne vient pas des techniques de développement de ces IA mais des organisations et des décisions managériales. En effet, il est toujours possible de trouver des solutions d'un point de vue technique, mais il est important pour les organisations de revoir les degrés d'autonomie et d'intégration des agents IA, ce qui permettrait de mieux appréhender les risques et de mettre en place des mesures de sécurité efficaces.

Solange GHERNAOUTI nous explique qu'en termes de cybersécurité, avant l'IA on ne savait pas bien faire, et avec l'IA on ne sait toujours pas bien faire. Le problème de compétence initiale de cybersécurité devait être substitué par des IA, cependant il manque encore les compétences pour piloter et maîtriser ces IA, donc le problème de base reste le même. Voici deux exemples de maîtrise qui seraient compliqués à mettre en place :

- Comment maîtriser les interactions entre les agents et faire en sorte que ces interactions ne soient pas des interactions pour plus de compromissions ?
- Comment maîtriser les accès des agents entre eux et en fonction des contextes ?

Les réponses de sécurité actuelles basées notamment sur le cloisonnement, le surveillance et le contrôle ne répondent plus au nouveau paradigme qu'introduit l'IA. Si nous n'avons aucun pouvoir d'action sur le modèle, nous n'aurons pas plus de sécurité. En tant qu'adopteur de ces solutions, nous n'aurons jamais de pouvoir d'action sur la conception du modèle, pouvant intégrer nativement des dysfonctionnements. Solange GHERNAOUTI souligne le fait que ce que nous appelons hallucination n'en est pas vraiment une, c'est en réalité un événements normal suivant la logique de conception du modèle sur lequel nous n'avons aucun visuel. Tous ces éléments montrent bien qu'il n'est pas possible pour une entreprise qui utilise l'IA de maîtriser tous ses risques.

Ainsi, Solange GHERNAOUTI nous cite plusieurs injonctions contradictoires, :

- Si on est rapide et intelligent, alors on a pas de sécurité ;
- Si on est intelligent et sécurisé, alors on a pas de rapidité ;
- Si on est rapide et sécurisé, alors on a des limitations dans les capacités de l'IA.

La sécurité a toujours besoin de limites mais l'IA efface les limites, donc ces deux paradigmes sont contradictoires.

Pour ce qui est de la notion de 0 trust, elle est incompatible avec le mode de conception des IA, pour la simple et bonne raison que nous ne pouvons pas faire confiance à la masse de données qui y sont injectées et pouvant être corrompues. En effet, l'IA est conçue pour ne pas respecter cette notion de 0 trust

Solange GHERNAOUTI nous explique ensuite que le savoir-faire en gestion des risques est complètement chamboulé par la façon de voir l'IA agentique comme des employés à part entière. Pour la confidentialité des données, nous savons faire de l'authentification et du chiffrement, pour la disponibilité des ressources nous savons faire de la redondance, mais nous ne savons pas maîtriser le contrôle de l'intégrité des systèmes d'IA. Ainsi nous relevons la problématique suivante : comment assurer l'intégrité des IA pouvant utiliser des données et des systèmes corrompus dont on développe la compromission à chaque fois que nous les utilisons ?

### 4 Point de vue de la société et de la biodiversité

Ce point de vue mène à la notion de monoculture numérique, c'est-à-dire une façon unique de faire de l'IA. Cette monoculture dictée par les États et les puissantes entreprises ayant le monopole sur cette technologie va évidemment mener à des problématiques de sécurité, mais surtout à une asymétrie entre ceux qui possèdent les capacités et les ressources pour mettre en place ces IA et ceux qui n'en ont pas.

Pour finir, Solange GHERNAOUTI commente les questions posées au sommet de l'IA à New Dehli :

- **Quelles sont les stratégies de résilience pour atténuer les risques posés par l'IA agentique tout en préservant l'innovation ?** Cette question montre qu'il n'y a pas de remise en question sur la finalité de l'IA et montre une volonté d'aller encore plus loin dans l'innovation. De plus, le terme de "résilience" n'est pas approprié car il fait référence à un échec de sécurité qui vise à survivre au problème de l'IA.
- **Que faire pour promouvoir la coopération pour la sécurité de l'IA au niveau international ?** Cette coopération à l'international est très compliquée aujourd'hui pour tout type de problématique.
- **Comment réguler le développement du déploiement et de l'usage de l'IA ?** Cette question montre la volonté d'avoir le moins de régulation possible pour avoir le plus de marge de manœuvre pour les États forts et les entreprises monopolisant les marchés de l'IA.

Enfin, Solange GHERNAOUTI met en avant encore une fois la complexité apportée par les innovations et l'évolution des IA agentiques, ainsi que la manière dont les problèmes sont seulement déplacés et qu'il n'y a pas de réflexion pour les régler.

## III Présentation du CESIN (Par Fabrice BRU)

Après la présentation de Solange GHERNAOUTI, Fabrice BRU prend la parole pour présenter le Club des Experts de la Sécurité de l'Information et du Numérique (CESIN) dont il est le président. Créé en 2012, le club rassemble aujourd'hui plus de 1300 membres, notamment des RSSI, des directeurs SSI, des responsables SOC et beaucoup d'autres, et permet d'offrir à ses membres un lieu d'échange dans lequel ils peuvent partager leur expérience et échanger sur leurs réflexions. La valeur principale portée par le CESIN est la solidarité entre ses membres, grâce à ce lieu d'échange et d'entraide entre les professionnels de la cybersécurité.

### 1 Les ambitions du CESIN

- Offrir un lieu d'échange, de partage d'expérience et de coopération aux experts de la sécurité de l'information et du numérique
- Favoriser les échanges entre experts et pouvoirs publics afin d'accompagner les évolutions réglementaires
- Participer à toute démarche nationale et internationale ayant pour objet la promotion de la sécurité de l'information et du numérique

— Faciliter les évolutions de l'entreprise en soutenant l'innovation grâce à la maîtrise des risques
— Favoriser l'émergence de solutions performantes et pragmatiques pour faire face aux risques auxquels sont confrontées les entreprises
— Sensibiliser usagers et décideurs aux enjeux de la sécurité de l'information

## 2 Les valeurs du CESIN

— **La convivialité :** Caractérisée par des moments informels comme des déjeuners, des apéros et tout autre moyen de mettre à l'aise les membres au sein du club.
— **La coopération :** Beaucoup de travaux sont réalisés avec le soutien de membres entre eux.
— **La confiance :** Respect de la confidentialité des échanges pour que les membres puissent s'exprimer librement.

## 3 Les fondamentaux du CESIN

Le fondement du CESIN repose sur les retours d'expérience entre les membres, dans le but d'améliorer le savoir-faire et la maturité, notamment dans un modèle de mentoring. De plus, c'est aussi un lieu de rencontre entre des RSSI de plusieurs entreprises partenaires. Fabrice BRU donne l'exemple de la supply chain et de la sous-traitance du numérique, qui est un vecteur de risque majeur, et au CESIN vous pouvez, en tant que RSSI, rencontrer le RSSI du fournisseur ou sous-traitant de votre entreprise, ce qui permet de faciliter les échanges.

## 4 Les membres

Il y'a 5 types de membres au sein du CESIN :
— **Les Fondateurs :** Qui ont mené à la création du CESIN
— **Les membres actifs :** Qui sont la communauté cyber active du club
— **Les associés :** Qui sont souvent des représentants des services de l'État (ANSSI, la police, etc.)
— **Les membres d'honneur :** Qui sont les anciens membres du CESIN, plus actifs, mais qui viennent apporter un regard extérieur, un recul et une vision stratégique.
— **Les sponsors :** Entreprises commerciales dont l'activité principale est la fourniture de solutions et/ou prestations en sécurité de l'information. Elles contribuent au financement du club.

Le président de CESIN nous a ensuite présenté le conseil d'administration, constitué de plusieurs responsables de la SSI de grands groupes et entreprises, ainsi que la mission de chaque membre dans le conseil.

## 5 Les moyens d'action

— Organisation de conférences tous les trimestres, portant sur des sujets de cybersécurité
— Organisation de réunion de travail, atelier one to one

— Publication du baromètre du CESIN, une enquête annuelle qui dresse l'état des lieux de la cybersécurité au sein des entreprises françaises via de nombreuses statistiques importantes.
— Université d'été d'environ 300 personnes permettant de se réunir et de réfléchir sur différentes thématiques
— Congrès à Reims tous les ans sur une thématique de cyber
— Parole d'expert : réunion d'1h30 dans laquelle un expert va décliner de bout en bout une thématique technique très précise.
— Réunion de communauté (4 communautés) :
  — communauté des grandes entreprises
  — communauté des PME
  — communauté des professionnels de la cyber dans l'industrie (OT)
  — communauté gestion de vulnérabilité

# IV Questions / Reponses

La session de questions/réponses a été entièrement menée par Solange GHERNAOUTI, portant toute sur sa présentation.

**Question sur la sécurité de l'utilisation de modèles d'IA (ChatGPT par exemple) en entreprise ?**

Le problème vient de l'orientation du modèle qui va intégrer la façon de voir la sécurité des données par les concepteurs qui peuvent être américains ou chinois par exemple. Il est donc compliqué de sécuriser un modèle que l'on ne maîtrise pas.

**Comment organiser concrètement la responsabilité, la traçabilité et l'auditabilité des systèmes d'IA agentique ? Et quelle sont les priorités pour sécuriser la couche d'orchestration et prévenir les effets de cascades entre agents et environnement critique ?**

Pour ces deux questions, Solange GHERNAOUTI affirme que ce sont des choses que nous ne savons pas faire aujourd'hui.

**Que conseillez vous à une entreprise qui digitalise ses services en utilisant l'IA ?**

Il faudrait réfléchir à ce que l'on perd en utilisant l'IA et à ce que nous pourrions faire sans l'IA en faisant autrement. Plus de facilité et plus de rapidité, mais à quel prix ?

**On a déjà du mal à maîtriser les risques d'architecture logiquement construite, comment maîtriser les conséquences de l'introduction d'agents dont on ne sait pas cerner les réponses ?**

C'est une contradiction majeure dans laquelle interviennent les promesses et les récits qui soutiennent l'idée que l'IA est devenue indispensable. Ainsi, Solange GHERNAOUTI nous explique que notre esprit a été colonisé par cette vision de voir les choses et que l'objectif est de reprendre le contrôle pour sortir de cette dépendance.

**Y a-t-il des structures d'échanges entre IA agentique dans les modèles d'orchestration que l'on a identifiés comme plus dangereux que d'autres ? A-t-on une typologie des modèles d'orchestrations plus risqués que d'autres ?**

Cela énonce un vrai problème, qui demande de questionner les modèles d'IA agentiques, car nous ne pouvons pas répondre à cette question.

**L'IA risque de bouleverser le modèle de commerce ?**

Oui car l'IA est bâtie sur un modèle de rentabilité et de surconsommation.

**Serait-il nécessaire de mettre en place une autorité régulatrice de l'IA ?**

Oui mais cela ne marchera pas pour l'instant. Ce sont les fournisseurs des IA qui s'autoproclament autorité régulatrice.