

Cyber & AI à l'horizon 2030 : la bataille pour la vitesse

Lettre des "Lundi de la cybersécurité" n° 90



Lundi 16 mars

18h00 - 20h00

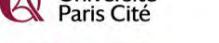
Bad AI



Cyber & AI à l'horizon 2030 : la bataille pour la vitesse



Pr Ahmed Mehaoua



1



Béatrice Laurent



Gerard Peliks

Cyber & Artificial Intelligence à l'horizon 2030

L’AI est de plus en plus utilisée par les outils de cybersécurité qui deviennent beaucoup plus efficaces pour contrer les attaques. Mais l’AI est aussi de plus en plus utilisée par les cyberattaquants pour passer à travers les défenses et perturber, voir, arrêter les systèmes d’information qu’ils agressent. Alors que deviendront la cybersécurité et la cybercriminalité dans quelques années ? Nul doute que le paysage du numérique ne sera plus celui qu’on connaît aujourd’hui.

Nous faisons appel à un expert en cybersécurité très connu, un futurologue qui s'est illustré depuis de nombreuses années par ses conférences, ses cours et ses diverses interventions dans l'industrie, Guy-
 

Philippe GOLDSTEIN que nous avions déjà fait intervenir dans notre « Lundi de la Cybersécurité » de décembre 2021 sur le sujet « *Cybersécurité, horizon 2035* ». Nous lui avions décerné le trophée du Néperon d'OR (constante de Néper ou nombre d'Euler : « e » tel que $\log e = 1$, avec $e = 2.71828\ldots$) environ. Nous avions compté 283 inscrits !



Pour le Lundi du 16 mars 2026, les inscriptions sont ouvertes.

Je donne la plume à GUY-Philippe GOLDSTEIN

Un train peut en cacher un autre. Alors que les autorités civiles de la cybersécurité à travers le monde mettent l'accent, à raison, sur le passage à la cryptographie post-quantique avec des calendriers qui s'étalent jusqu'en 2035, une autre menace aussi puissante est en train en parallèle de voir le jour et d'émerger très rapidement.

Le Hacker Agentique Autonome, capable de rivaliser avec la crème de la crème des hackers humains, semblait encore de l'ordre de la science-fiction et des horizons lointains il y a 18 mois. Il est désormais en train de prendre vie de manière très concrète. De la capacité à opérer des manœuvres latérales ; à celles de se retrouver en tête des classements de bug bounty ou de concours « Capture The Flag » ; à l'identification de vulnérabilités nouvelles voir la capacité de mener à 80-90% des campagnes avancée d'espionnage de manière autonome, les démonstrations de capacités se sont succédées tout au long de 2025.

Prises ensemble, elles forment la base d'une alerte qui doit concerner tous les acteurs de la cybersécurité – conclusion qu'ont commencé à tirer à partir d'octobre 2025 une suite d'experts internationaux.

- Mais à quoi pourrait ressembler ce nouveau monde de la cybersécurité offensive à l'âge des hackers agentiques ?
- Comment pourrait se transformer les différentes phases de l'attaque, de l'ingénierie sociale augmentée à l'exploitation, passée la phase d'intrusion ?
- Quels nouveaux types d'approches devront être explorées pour renforcer la cybersécurité des systèmes IT ?
- Et quelles seront les nouvelles composantes de la gouvernance de la cybersécurité à l'âge de l'IA agentique ?

Telles sont toutes les pistes qui seront abordés dans ce talk prospectif.

Qui est GUY-Philippe GOLDSTEIN ?



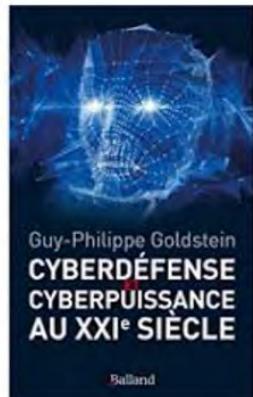
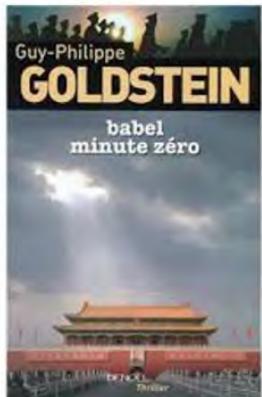
Guy-Philippe Goldstein est enseignant à l'Ecole de Guerre Economique ; advisor pour PwC sur les questions d'IA et de cybersécurité ; et advisor pour certains fonds VC sur les sujets cyber. Ses travaux et publications ont abordé entre autres les questions de prospectives sur l'évolution de la cybersécurité ; le coût des incidents cyber ; la lutte contre la guerre cognitive ; et la manière dont l'IA va changer les modes de productions et de management.

Il est déjà intervenu sur ces sujets lors des conférences TEDGlobal, TEDxParis et TEDxAthens ainsi qu'au FIC ou encore à CyberWeek et CyberTech en Israël.

Il est également l'auteur de **Babel Minute Zéro**, un roman d'anticipation publié en 2007, évoquant un scénario de conflit entre la Chine et les Etats-Unis pour le contrôle de Taiwan se déroulant dans le Cyberespace, et qui a été lu par de nombreux responsables militaires en

France et au plus haut niveau du gouvernement israélien lors de l'accélération du programme cyber au début des années 2010.

Voici des livres de Guy-Philippe qui vous montrent le savoir-faire du personnage :



Demande d'inscription au lundi 16 mars, par visio-conférence à partir de 18 h 00.



Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique. Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, un lien pour entrer dans la visioconférence Zoom.

Les demandes d'inscriptions sont à adresser à **Béatrice Laurent** co-organisatrice de nos évènements :

beatricelaurant.CDE@gmail.com

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux intervenants. Si vous voulez être ajoutés à ma liste de distribution des lettres des « *Lundi de la cybersécurité* » mensuels, demandez-le-moi par mail (gerard.peliks@noos.fr).

Si vous vous inscrivez pour assister à notre évènement, soyez connectés le **lundi 16 mars, dès 18 h 00 ou mieux, un peu avant**. La salle d'attente Zoom sera ouverte aux alentours de **17 h 00** pour des conversations informelles entre intervenants et participants. Ce sont toujours d'agréables échanges qui se font avant 18 h 00.

Quelques minutes avec une association : CyberEdu



Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé des intervenants et la session questions / réponses, qui commence autour de 19 h 30, nous donnons pour une quinzaine de minutes la parole à une organisation ou à une personne qui opère dans l'écosystème du numérique et dans la sécurité de l'information.

Cette séquence des « quelques minutes avec une association » sera animée par **Julien BREYAUT, président de CyberEdu**, membre des GT formation du club EBIOS et du Campus Cyber, enseignant en cyberdéfense à l'École Nationale Supérieure d'Ingénieurs de l'Université Bretagne Sud (ENSIBS Vannes).

"CyberEdu, association créée sur l'initiative de l'ANSSI, œuvre depuis 2016 à ses côtés pour accompagner les formations dans l'intégration de compétences cyber dans les programmes de formation. Lorsque cette intégration est satisfaisante, c'est à dire contextualisée aux métiers, les formations peuvent être labellisées et utiliser ce label dans leurs communications et leurs diplômes.

Les principales formations nationales en informatique ont été accompagnées et labellisées (BTS SIO et CIELL, BUT informatique et R&T, AFPA...). L'association contribue aux initiatives nationales autour des compétences et métiers Cyber avec par exemple :

- la création de matrices de compétences au sein du GT formation du Campus Cyber national,
- l'accompagnement des AMI CMA Cyber (dont la féminisation des métiers Cyber avec "FEMA" de Social Builder)"

Le coin des « Lundi de la cybersécurité » précédents.

Vous trouverez, sur le web de l'ARCSI – Association des Réservistes du Chiffre et de la Sécurité de l'Information :

https://www.arcsi.fr/evt_passes.php

tous les détails, slides, parfois aussi les enregistrements et des comptes rendus de nos « Lundi ».

Par exemple, pour le « Lundi de la Cybersécurité » de janvier :

La lettre d'invitation est [disponible ici](#).

Les slides de la présentation "Le monde numérique aime-t-il vraiment les enfants" de Diane RAMBALDINI sont [disponibles ici](#).

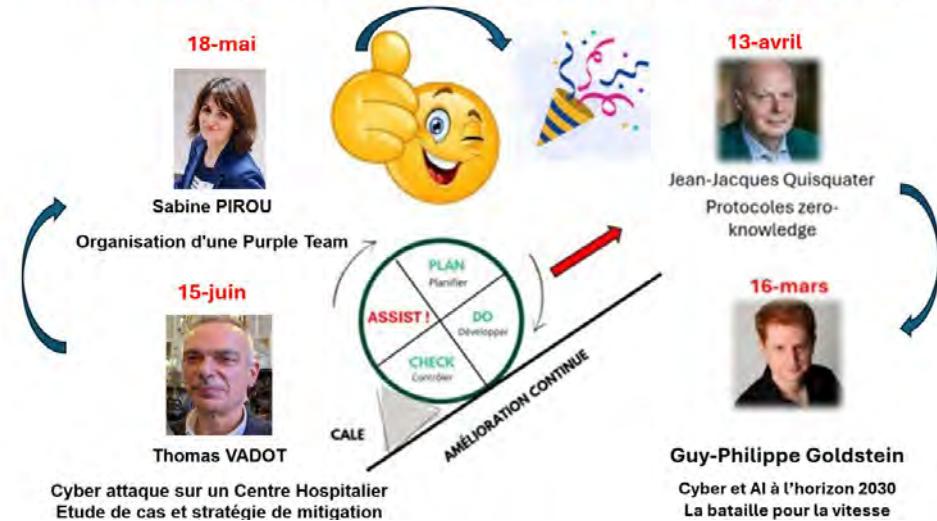
La rediffusion du Lundi de la Cybersécurité de janvier 2026 est [disponible ici](#).

Le compte-rendu est [disponible ici](#).

Le coin des « Lundi de la cybersécurité » suivants.

Nous commencerons avec Guy-Philippe en mars, suivi de Jean-Jacques en avril, puis Sabine en mai, et Thomas en juin.

Nos « Lundi de la Cybersécurité » de mars à juin 2026



C'est quoi cette roue qui monte, qui monte, qui monte ? ...

La norme ISO27001 définit comment un Système d'Information doit être protégé, et illustre les processus par le sigle PDCA, Plan, Do, Check, ACT, symbolisé par la roue de Deming qui vous fait monter, à chaque tour, une pente vers plus de cybersécurité.

On planifie ce qu'il faut faire, on le fait, on mesure les écarts entre ce qu'on aurait dû faire et ce qu'on a réellement fait, et on réalise ce qu'on aurait dû faire. Ensuite on continue le processus.

La roue de Deming a alors fait un tour complet qui lui fait à fait monter la pente. On place une cale pour garder l'acquis et éviter que la roue ne redévale la pente vers une cybersécurité moins constructive.

Dans cette roue de Deming, j'ai juste changé le sigle « ACT » par le sigle « ASSIST ».

Donc PDCA : Plan, Do, Check, Assist.

- Plan : On décide d'assister à notre prochain « Lundi de la Cybersécurité ».
- Do : On inscrit ce prochain Lundi dans son calendrier, et on demande son inscription par mail à beatrice.laurent.cde@gmail.com.
- Check : On se rend compte que la semaine du Lundi du mois approche, et qu'on est disponible ce lundi-là, de 18h00 à 20h00.
- Assist : On assiste à ce Lundi de la Cybersécurité.

Et on place la cale pour poursuivre sa présence aux « Lundi de la Cybersécurité » en attendant dès le lendemain du Lundi du mois en cours, l'annonce de l'ouverture des inscriptions pour le Lundi de la Cybersécurité du mois suivant. La cale, c'est bien sûr votre calendrier à remplir.

Le coin-coin de l'IA Générative



Allons-nous obtenir une « hallucination » ou une réponse qui décrit une situation bien réelle ?

Prompt posé à Gemini :

Qui gagnera la course de l'Intelligence Artificielle ? Les cyberattaquants ou les cyberdéfenseurs ?

Réponse de Gemini :

C'est le nouveau front de cette guerre numérique. Si l'on regarde l'évolution actuelle, l'Intelligence Artificielle ne change pas la nature du conflit, mais elle en accélère radicalement la **vitesse et l'échelle**.

Voici comment le match se joue avec ce nouvel arbitre qu'est l'IA :

1. Le sprint des attaquants : L'industrialisation du chaos

Pour les attaquants, l'IA est un multiplicateur de force. Elle permet de transformer des attaques artisanales en opérations de masse.

- **Le Phishing "parfait"** : Fini les fautes d'orthographe et les syntaxes douteuses. L'IA générative crée des emails de phishing ultra-personnalisés et crédibles dans n'importe quelle langue.
- **Les Deepfake** : L'IA permet d'imiter la voix d'un PDG lors d'un appel (fraude au président) ou de simuler son visage en visioconférence.
- **Le code malveillant auto-généré** : Même un pirate débutant peut utiliser des modèles de langage pour générer des scripts d'exploitation de vulnérabilités, abaissant ainsi la "barrière à l'entrée" du cybercrime.

2. La riposte des défenseurs : L'hyper-vigilance

Pour les défenseurs, l'IA est le seul moyen de ne pas être submergé par le déluge de données.

- **L'analyse comportementale** : Là où un humain mettrait des jours à repérer une anomalie, une IA détecte en quelques millisecondes qu'un compte utilisateur se comporte de manière inhabituelle (ex : connexion à une heure inhabituelle depuis un nouvel endroit).
- **La réponse automatisée** : L'IA peut isoler un ordinateur infecté du reste du réseau instantanément, avant même qu'un analyste humain n'ait fini de lire l'alerte.
- **La chasse aux vulnérabilités** : Les entreprises utilisent l'IA pour scanner leur propre code et colmater les brèches avant que les pirates ne les trouvent.

Qui a l'avantage ?

Le combat se résume à une équation de **temps** et de **coût** :

Facteur	Impact de l'IA sur l'Attaque	Impact de l'IA sur la Défense
Vitesse	Gagnant. L'attaque est lancée en quelques secondes.	Suiveur. Doit réagir en temps réel.
Échelle	Peut cibler des millions de personnes à la fois.	Protège des infrastructures entières d'un coup.
Coût	Réduit drastiquement le coût d'une attaque complexe.	Coûteux à mettre en place (talents, serveurs).

Le constat est direct : À court terme, l'IA favorise les **attaquants**, car elle leur offre des outils de pointe pour un investissement minime. À long terme, elle favorise les **défenseurs** qui disposent de plus de données pour "entraîner" leurs systèmes de protection à devenir quasi impénétrables.

Le verdict

Ce n'est pas une course avec une ligne d'arrivée, mais une **course de haies infinie**.

Le vrai gagnant sera celui qui saura le mieux collaborer avec la machine. L'humain seul est trop lent ; l'IA seule est trop rigide. La victoire appartient à ceux qui maîtriseront le "**Centaure Security**" : l'alliance de l'intuition humaine et de la puissance de calcul de l'IA.

Bon, OK et nous écouterons **GUY-Philippe GOLDSTEIN** nous dire ce qu'il en pense.

Inscrivez-vous (mail à beatricelaurent.cde@gmail.com) ou cliquez sur le rectangle rouge :

JE M'INSCRIS

Gérard