








## Keynote Speaker: Carole House – French Summary and Transcript

(Note: This transcript was AI-generated using [NoteGPT](#). Transcripts may include inconsistencies or errors and some sentences have been condensed.)





### Résumé

Carole House souligne l'importance de la cybersécurité et de l'inclusion financière, en mettant en avant leur lien dans les efforts de sécurité nationale.

### Points clés

-  Carole House est conseillère spéciale en cybersécurité à la Maison Blanche.
-  L'inclusion financière est essentielle pour la stabilité du marché et la protection des consommateurs.
-  Une identité numérique solide est cruciale pour prévenir l'exploitation dans les systèmes financiers.
-  L'IA et les actifs numériques présentent à la fois des opportunités et des risques pour la cybersécurité.
-  Les initiatives gouvernementales se concentrent sur la promotion d'un accès sécurisé aux services financiers.
-  Les menaces en cybersécurité nécessitent des solutions robustes de gestion des identités.
-  La collaboration entre le gouvernement et l'industrie est vitale pour traiter des problèmes complexes.

### Aperçus clés

-  L'inclusion financière est liée à la sécurité nationale, soulignant le besoin d'un accès sécurisé aux services. À mesure que de plus en plus de citoyens effectuent des transactions numériques, le risque d'exploitation augmente, nécessitant une approche ciblée pour protéger les consommateurs.
-  Les solutions d'identité numérique sont cruciales pour lutter contre la cybercriminalité. Un cadre d'identité solide peut atténuer les risques associés à la fraude, renforçant l'importance de méthodes d'identification sécurisées dans les écosystèmes financiers.
-  L'essor de la technologie IA pose de nouveaux défis pour la cybersécurité. Bien que l'IA démocratise l'accès à des outils sophistiqués, elle permet également aux cybercriminels d'exploiter ces avancées à des fins malveillantes.
-  Des cadres de gestion des risques efficaces sont nécessaires pour tirer parti des nouvelles technologies. Le gouvernement vise à établir des lignes directrices qui

garantissent un développement responsable de l'IA tout en protégeant les consommateurs et les systèmes financiers des menaces évolutives.

- 🖥️ Les mesures de cybersécurité doivent évoluer avec les avancées technologiques. La mise en œuvre de l'authentification multi-facteurs et d'autres solutions de gestion des identités peut réduire considérablement les vulnérabilités dans les transactions financières.
- 🤝 La collaboration entre le gouvernement et l'industrie est essentielle pour aborder les complexités de l'inclusion financière et de la cybersécurité. Des dialogues continus aideront à identifier et à mettre en œuvre des solutions innovantes à ces défis entremêlés.
- 🚀 L'avenir des services financiers dépend de pratiques sécurisées et inclusives. En priorisant la cybersécurité dans les efforts d'inclusion financière, nous pouvons favoriser un paysage financier plus sûr et plus équitable pour tous.

## Transcript

00:15

Salut, je suis Carole House. Je travaille comme conseillère spéciale pour la cybersécurité et les infrastructures critiques au Conseil de sécurité nationale de la Maison Blanche. Je viens tout juste de revenir au NSC après quelques années hors du gouvernement, mais j'ai déjà occupé divers postes, en étant vraiment à l'intersection de l'exploitation de la technologie et des objectifs de sécurité nationale, au Trésor américain sur la colline. J'ai fait trois missions à la Maison Blanche et avant ça, j'étais capitaine dans l'armée américaine. Donc d'abord, je veux juste remercier.

00:43

Le centre pour l'inclusion financière a l'honneur de parler aujourd'hui d'un sujet aussi crucial qui est au cœur de nombreux efforts en cours au sein du gouvernement américain. Avant de plonger dans les super initiatives que nous avons mises en place, je voudrais d'abord expliquer pourquoi je parle de ce sujet au Conseil de sécurité nationale. Il y a beaucoup de résultats et d'équités que nous souhaitons pour notre système financier, allant de la stabilité du système financier et des marchés à la protection des consommateurs.

01:13

Des protections contre les criminels financiers et les blanchisseurs d'argent, tout en promouvant notre leadership en innovation technologique et en renforçant notre rôle central dans le système financier mondial. L'inclusion financière a un impact direct sur

chacun de ces objectifs, et elle est aussi directement influencée par eux. Donc, des domaines de la sécurité nationale comme la lutte contre le blanchiment d'argent et le financement du terrorisme ne sont pas des objectifs qu'on vise dans le vide, et l'inclusion financière n'est pas poursuivie sans tenir compte de nombreux autres facteurs. Au contraire, ces domaines sont alignés.

01:46

Dans une vision commune de soutien mutuel pour offrir un accès inclusif aux consommateurs à des biens et services financiers sûrs, abordables et sécurisés, en faisant de l'inclusion financière un pilier de notre sécurité nationale et économique, je vais maintenant parler de l'importance de la technologie. Certains de nos efforts pour promouvoir la sécurité et la confiance dans le cyberspace sont également cruciaux pour cette inclusion financière, car, comme on l'a dit, l'inclusion dans un système qui n'est pas...

02:16

Il faut mettre en place des garde-fous nécessaires pour éviter que les consommateurs ne soient exploités pour leurs données, ou qu'ils soient victimes de cybercriminels ou d'autres acteurs malveillants. Ce n'est pas du tout le genre de résultat qu'on souhaite pour l'inclusion financière dans nos systèmes. Comme je l'ai dit, on devient de plus en plus dépendants et imbriqués avec cette technologie. On ne fait pas marche arrière niveau numérisation, au contraire, ça augmente. Du coup, on doit trouver des moyens pour que ces technologies offrent un accès à grande échelle.

02:47

« Les services et l'accès démocratisé à ces services pour les citoyens, ça inclut aussi cet accès démocratisé pour les acteurs impliqués. On doit s'assurer qu'on utilise ces technologies de manière positive pour éviter que les acteurs malveillants n'exploitent les bons acteurs. Et puis, il faut continuer à créer des opportunités économiques à grande échelle et à garantir un accès inclusif pour les Américains et d'autres citoyens à travers le monde. D'abord, je vais parler de l'identité numérique, un sujet sur lequel je travaille depuis des années, depuis que j'étais au ministère des Finances, à la tête de nos efforts en matière d'identité. »

03:19

L'identité est un enjeu crucial. L'innovation rapide sur Internet, les téléphones mobiles et d'autres technologies numériques a apporté une commodité et une efficacité sans précédent aux Américains au quotidien. Cependant, quand ces mêmes citoyens

interagissent avec le monde physique en ligne, l'expérience est souvent pleine de frictions et d'opportunités d'exploitation. Donc, le manque d'une identité numérique solide aggrave cette friction. Avec la croissance continue des paiements numériques, du commerce et des interactions en ligne, il y a un besoin et une opportunité croissants pour...

03:50

Promouvoir le développement de solutions d'identité solides qui offrent aux consommateurs un moyen facile, sécurisé, abordable et fiable de s'identifier eux-mêmes et leurs partenaires dans les systèmes numériques. L'identité, c'est vraiment un sujet complexe, tout comme tout ce qui touche à l'inclusion financière, qui est une question très compliquée et dynamique, avec des implications pour la cybersécurité, la croissance économique, la vie privée, et la liste continue. C'est pour ça que des dialogues comme ceux qui se tiennent cette semaine entre le gouvernement et l'industrie sont indispensables pour examiner tout ça.

04:22

Les différents aspects de l'identité et d'autres problèmes technologiques complexes jouent un rôle central dans beaucoup des efforts de cybersécurité qu'on a mis en place dans l'administration, et c'est bien justifié. Beaucoup d'incidents cybernétiques impliquent des vecteurs de compromission qui auraient pu être évités grâce à des solutions de gestion d'identité et d'accès plus robustes, comme l'implémentation de solutions d'authentification multifacteur. On a aussi constaté que les faiblesses des solutions d'identité sont responsables d'une grande partie de la cybercriminalité, y compris des crimes financiers facilités par le numérique.

04:54

comme la fraude à l'identité synthétique qui contrecarrent la vérification d'identité, les prises de contrôle de comptes qui exploitent les faiblesses dans l'authentification d'identité, et la fraude par compromission d'email professionnel qui cible les faiblesses dans les processus d'autorisation et de vérification entre partenaires de confiance. On a entendu des estimations de la part des acteurs du secteur que la grande majorité des incidents de ransomware auraient pu être évités simplement en mettant en place des solutions d'authentification à plusieurs facteurs (MFA). L'identité est aussi au cœur du modèle de sécurité "zero trust".

05:25

Des mises en œuvre, c'est un peu une stratégie ou une approche en cybersécurité qui consiste à supposer que tes réseaux ont été compromis. Ça garantit que tu donnes un

accès minimal aux infos critiques et sensibles. Tout ça, ça revient à l'inclusion financière dans les écosystèmes numériques, ce qui nous oblige à réfléchir à comment mettre en place de bonnes pratiques d'identité pour éviter les abus tout en favorisant cette inclusion, histoire d'assurer la sécurité.

05:55

et garantir l'inclusion financière aussi euh dans mon ancien poste euh quand j'étais dans l'industrie, euh où je suis récemment revenu pour le gouvernement, j'ai été président de la Commodity Futures Trading Commission aux États-Unis, euh président du comité consultatif sur la technologie, euh et j'y ai contribué en tant que président à deux rapports qu'on a publiés sur des questions d'intelligence artificielle ainsi que sur des actifs numériques. Euh aussi dans mon rôle à la Maison Blanche, j'ai soutenu des efforts sur...

06:25

La sécurité de l'intelligence artificielle et le développement responsable des actifs numériques comme les cryptomonnaies et les monnaies numériques de banques centrales soulignent un changement de paradigme vers la décentralisation et un accès démocratisé aux technologies vraiment intéressantes et innovantes. On assiste à un accès démocratisé à des technologies super sophistiquées, comme on l'a vu avec l'arrivée de ChatGPT et de Llama, ainsi que d'autres modèles de langage très avancés. Cela pousse à aller de l'avant.

06:56

une opportunité incroyable, euh, dans l'économie, c'est aussi, du point de vue de la sécurité nationale, ça pourrait offrir des opportunités d'accès incroyablement démocratisées pour des acteurs malveillants comme les cybercriminels. Donc, euh, la capacité des groupes de cybercriminalité à tirer parti de cette technologie super sophistiquée pour mener des campagnes de fraude généralisées et des activités dans l'écosystème de la cybersécurité et de la cybercriminalité, c'est vraiment une grande préoccupation pour nous. Par exemple, certaines des méthodes majeures qu'on avait conseillées aux institutions financières quand j'étais là.

07:29

On doit lutter contre les fraudes comme le business email compromise. On leur a conseillé d'instaurer un processus d'autorisation en plusieurs étapes, en dehors des canaux habituels, pour les transactions de grande valeur. Mais avec l'accès de plus en plus répandu et la capacité de créer des deepfakes super sophistiqués, il devient presque facile de contourner ces contrôles pour se protéger, soi et son institution, contre la fraude. C'est

presque devenu n'importe quoi pour des cybercriminels de moins en moins malins, grâce à l'IA qui facilite tout ça.

08:03

Les capacités deviennent beaucoup plus accessibles, donc c'est là que le gouvernement des États-Unis, à travers des initiatives comme la création de notre Institut de sécurité de l'IA au NIST, ainsi que d'autres efforts en cours à travers le gouvernement américain, cherche des moyens de promouvoir le développement sûr et responsable des technologies d'IA. On veut aussi s'assurer qu'on puisse utiliser et tirer parti de l'IA à la vitesse, à l'échelle et avec la sophistication nécessaires pour adapter des choses comme les cadres de gestion des risques et les évaluations de risques.

08:32

On ne prend pas des décisions arbitraires comme le fait de regrouper des catégories de personnel, mais on peut aussi utiliser la technologie pour lutter contre la fraude omniprésente. Donc, tout ça fait partie des mesures que nous avons mises en place au sein du gouvernement américain pour promouvoir un accès sûr et sécurisé aux services financiers. C'est à l'intersection de la sécurité nationale et des objectifs d'inclusion financière. Je suis vraiment honoré d'avoir eu l'occasion de vous parler et des échanges qu'on a eus.

09:01

C'est incroyable ce qui se passe cette semaine, euh, je vous remercie encore beaucoup pour l'opportunité et l'honneur de vous parler à tous.