

Assurer l’avenir : entretien avec Jen Easterly sur la cyberrésilience, la confiance et le leadership dans un monde numérique

15 mai 2025, 12:01

Ann Debaere

Dans un monde où les bouleversements sont inévitables, la résilience n’est pas une option. Elle est essentielle. Peu de dirigeants en ont une meilleure compréhension que Jen Easterly, ancienne directrice de l’Agence de cybersécurité et de sécurité des infrastructures (CISA, de l’anglais Cybersecurity and Infrastructure Security Agency) des États-Unis et officière de l’armée décorée. À l’approche de son intervention lors de Securing Tomorrow. Now., l’événement annuel d’Agoria et de Sirris qui se tiendra le mercredi 4 juin à Skyhall (Aéroport de Bruxelles), nous avons échangé avec Jen Easterly sur le leadership, la cyberrésilience, le rôle de l’Europe dans la sécurité mondiale, et les adaptations nécessaires des entreprises face à un avenir numérique instable.

Forte de votre expérience militaire et dans le renseignement, quelles leçons en matière de résilience s’appliquent directement aux dirigeant·es d’entreprise ?

Jen Easterly: L’une des leçons les plus importantes, c’est que la résilience ne consiste pas simplement à rebondir — mais à rebondir vers l’avant. Il s’agit de développer la capacité à encaisser les chocs, à s’adapter sous pression et à en sortir plus fort.

Cela demande bien plus que de la préparation : cela requiert du leadership, de la confiance et une culture d’entreprise solide. On ne peut pas empêcher tous les bouleversements. La résilience, c’est accepter cette réalité et se préparer à répondre et à se relever avec détermination — grâce à des équipes entraînées, des systèmes résilients et un état d’esprit guidé par une mission claire.

Comment évaluez-vous les efforts de l’Europe pour faire face aux



Jen Easterly, Former Director, U.S. Cybersecurity and Infrastructure Secure Agency

Jen Easterly: Le cyberespace n’a pas de frontières, et l’Europe a accompli des avancées significatives, notamment en matière de réglementation sur la vie privée et d’harmonisation des politiques cyber. Mais le paysage des menaces évolue plus vite que les politiques ou les structures administratives ne peuvent le suivre.
Nous avons besoin de rapidité, d’audace et de collaboration — en particulier de partenariats public-privé transfrontaliers. Puisque les menaces sont mondiales, nos défenses doivent l’être aussi.

Existe-t-il, selon vous, des scénarios de menace encore sous-estimés par les dirigeant·es, notamment en Europe ?

Jen Easterly: Oui — en particulier les menaces stratégiques et à long terme émanant d’États-nations comme la Chine et la Russie. Les cybercriminels sont dangereux, mais les acteurs étatiques représentent un risque encore plus élevé. Aux États-Unis, nous avons constaté que des acteurs chinois s’implantaient discrètement dans des secteurs d’infrastructures critiques.
Par ailleurs, l’intelligence artificielle constitue un vecteur de risque majeur — en facilitant des cyberattaques plus sophistiquées, la création de deepfakes et la diffusion de désinformation. Ces

risques ne sont pas théoriques : ils sont déjà bien réels.

Durant votre mandat à la CISA, vous avez mené une transformation en profondeur. Comment avez-vous modernisé l'agence ?

Jen Easterly: Lorsque j'ai rejoint la CISA, c'était une agence encore jeune, confrontée à d'importantes pénuries de personnel — environ 1 000 postes vacants. Il fallait renforcer rapidement nos capacités et nos compétences.
Au-delà de la simplification du recrutement, la véritable transformation a été culturelle. Nous avons instauré une culture axée sur la mission et centrée sur l'humain, capable d'attirer des talents techniques de haut niveau, mais aussi collaboratifs. La confiance — en interne comme avec nos partenaires — en a été la pierre angulaire.

Quelle mesure concrète avez-vous mise en place pour attirer les meilleurs talents ?

Jen Easterly: Pendant mon mandat, nous avons recruté plus de 2?200 personnes — non seulement des experts techniques, mais aussi des profils collaboratifs. Nous avons mis l'accent sur la création d'un environnement de travail où les gens se sentent responsabilisés, valorisés et investis dans une mission plus grande qu'eux. Dans un marché concurrentiel, la culture a fait toute la différence.

Les citations les plus importantes de Jen Easterly

- « La résilience, ce n'est pas seulement rebondir. C'est rebondir vers l'avant. »
- « On ne se fait pas un ami en pleine crise. La confiance doit se construire en amont. »
- « En cybersécurité, il est temps d'arrêter de glorifier les attaquants et de commencer à exiger des comptes des fournisseurs. »
- « La sécurité ne doit pas reposer sur les utilisateurs. Elle doit être intégrée dès la conception. »
- « L'avenir appartient à celles et ceux qui osent le façonner. Et l'avenir se sécurise dès aujourd'hui. »
- « Une bonne hygiène numérique permet de prévenir jusqu'à 98 % des attaques. Ce sont les bases qui comptent le plus. »

Quelles leçons tirées de la CISA, comme le Joint Cyber Defense Collaborative, pourraient être appliquées en Belgique ou en Europe ?

Jen Easterly: Nous avons créé le Joint Cyber Defense Collaborative (JCDC) pour décloisonner les agences de renseignement, les forces de l'ordre et les services de cyberdéfense, et pour collaborer directement avec le secteur privé.

Cette collaboration opérationnelle et en temps réel s'est révélée essentielle lors de crises comme la faille Log4j ou l'invasion russe de l'Ukraine. Depuis, le Canada a créé sa propre version de ce modèle. Je suis convaincue que l'Europe pourrait en tirer parti, non seulement au niveau national, mais aussi à l'échelle de l'Union européenne.

Comme je le dis souvent : on ne se fait pas un ami en pleine crise. La confiance et la coopération doit se construire en amont.

Comment la coopération internationale devrait-elle évoluer pour répondre à la nature transfrontalière des cybermenaces ?

Jen Easterly: Nous avons besoin d'une collaboration opérationnelle en temps réel, et non simplement d'alliances sur le papier. Aux États-Unis, la cybersécurité a été élevée au rang de priorité de sécurité nationale, avec un engagement fort des dirigeants et des moyens financiers conséquents.
L'Europe dispose de nombreux atouts, mais elle bénéficierait d'un effort plus unifié entre les capacités nationales. Une approche intégrée à l'échelle de l'UE, étroitement liée aux États-Unis et à leurs alliés, sera essentielle pour assurer la cyberdéfense de demain.

Vous êtes une fervente défenseuse du mouvement « Secure by Design ». Que devraient faire les entreprises du numérique différemment aujourd'hui ?



Jen Easterly: Nous avons tendance à glorifier les attaquants, comme Volt Typhoon, et à blâmer les victimes pour ne pas avoir mis à jour leurs systèmes — mais nous devons changer de perspective et demander des comptes aux fournisseurs de technologies.
La sécurité doit être un élément central de la conception, une priorité dès le premier jour pour les PDG, les conseils d'administration et les équipes produit. Trop souvent, on privilégie la rapidité de mise sur le marché ou la réduction des coûts au détriment de la sécurité — cela doit changer.
Nous avons lancé un engagement « Secure by Design », déjà signé par plus de 300 entreprises. L'Europe montre l'exemple avec des initiatives comme le Cyber Resilience Act, qui imposent des normes de sécurité plus élevées et plus rapidement que les États-Unis.
Aujourd'hui, personne n'achèterait une voiture sans ceintures de sécurité. De la même façon, nous ne devrions pas accepter des produits numériques dépourvus de protections de base intégrées.

Comment les entreprises manufacturières peuvent-elles mieux concilier innovation et cybersécurité ?

Jen Easterly: L'innovation est essentielle, mais la sécurité doit être intégrée dès le départ. Les entreprises manufacturières doivent identifier leurs « actifs stratégiques » — les systèmes et données critiques — et les protéger par des défenses en couches et une segmentation des réseaux.
Trop souvent, la cybersécurité est perçue comme une simple assurance. Elle doit au contraire être considérée comme un investissement stratégique, au même titre que l'innovation et la productivité. Les entreprises doivent tirer parti de leur pouvoir d'achat pour exiger un meilleur niveau de sécurité de la part de leurs fournisseurs.

Pour les petites entreprises qui ne disposent pas des ressources des grandes structures, quelles sont les trois priorités en matière de cybersécurité ?

Jen Easterly:

1. **Installer les mises à jour :** De nombreuses attaques exploitent des vulnérabilités connues qui pourraient être corrigées simplement par une mise à jour.
2. **Utiliser des mots de passe robustes et un gestionnaire de mots de passe :** Des mots de passe uniques et solides sont essentiels.
3. **Réfléchir avant de cliquer :** Former les employé·es à être vigilants face aux e-mails, SMS et appels suspects.

Il faut également activer l'authentification multifacteur (MFA). Ces gestes de base — l'hygiène numérique — peuvent permettre d'éviter jusqu'à 98 % des attaques.

Quelles mesures concrètes les dirigeant·es peuvent-ils prendre pour intégrer la cybersécurité dans l'ensemble de leur organisation ?

Jen Easterly:

- **Rendre la cybersécurité personnelle :** Relier les comportements aux risques concrets à travers des récits parlants, plutôt que par la peur.
- **Donner l'exemple au sommet :** Les PDG et les conseils d'administration doivent considérer la cybersécurité comme une responsabilité de leadership, et non comme un simple sujet informatique.
- **Valoriser la sécurité :** Reconnaître et récompenser les bonnes pratiques en matière de cybersécurité dans toute l'organisation.

Il s'agit d'un changement culturel — et les dirigeant·es doivent incarner ce qu'ils prônent.

Enfin, pourquoi les dirigeant·es d'entreprise belges devraient-ils assister à « Securing Tomorrow. Now. » et écouter votre keynote ?

Jen Easterly: Parce que l’avenir se construit dès aujourd’hui, et qu’il appartient à celles et ceux qui ont le courage de le façonner. Les menaces sont urgentes, mais l’opportunité de construire un monde numérique plus sûr et plus solide l’est tout autant.

À Bruxelles, je partagerai des leçons tirées du terrain, sur le leadership, la résilience et la sécurisation de notre avenir. Je ne viens pas simplement pour informer ; je viens pour inspirer.

Auteurs



Ann Debaere