



AFRICA CENTER FOR STRATEGIC STUDIES

PRIORITÉS EN MATIÈRE DE SÉCURITÉ DU CYBERESPACE POUR LES ACTEURS DE LA SÉCURITÉ NATIONALE EN AFRIQUE

NOTE D'INFORMATION

QUOI : Le Centre d'Études Stratégiques de l'Afrique organisera un programme virtuel de quatre semaines pour examiner le rôle des acteurs de la sécurité nationale dans la réponse aux défis de la sécurité du cyberspace en Afrique. Ce programme examinera comment le secteur de la sécurité peut coopérer avec les autres parties prenantes des secteurs public et privé pour faire face aux menaces croissantes liées à la cybernétique sur le continent. Les participants ayant complété le programme recevront un certificat reconnaissant leur accomplissement.

Les objectifs du programme sont les suivants :

1. Améliorer la compréhension des menaces et des défis de la sécurité du cyberspace en Afrique.
2. Identifier les priorités que les acteurs africains de la défense et de la sécurité doivent prendre en compte lorsqu'ils se préparent et répondent à des activités cybernétiques malveillantes.
3. Comparer les expériences, les perspectives et les bonnes pratiques en matière de politique de sécurité du cyberspace entre un éventail de parties prenantes du secteur de la sécurité, du secteur civil, du secteur privé et des organisations non gouvernementales.

OÙ : En ligne, via Zoom for Government

QUAND : 3-4 août 2021
10-11 août 2021
17-18 août 2021
24-25 août 2021

QUI : Des participants ayant une vaste expérience dans le secteur de la sécurité, du gouvernement, du secteur privé et de la société civile seront invités à participer. Les pays suivants sont invités à désigner des participants : Algérie, Angola, Bénin, Botswana, Burkina Faso, Burundi, Cabo Verde, République centrafricaine, Tchad, Comores, Congo, République démocratique du Congo, Côte d'Ivoire, Djibouti, Égypte, Eswatini, Gabon, Gambie, Ghana, Guinée, Guinée-Bissau, Kenya, Lesotho, Liberia, Libye, Madagascar, Malawi, Mali, Mauritanie, Maurice, Maroc, Mozambique,

Namibie, Afrique du Sud, Niger, Nigeria, Rwanda, Sao Tomé-et-Principe, Sénégal, Seychelles, Sierra Leone, Somalie, Soudan, Tanzanie, Togo, Tunisie, Zambie. Chaque pays est invité à nommer trois participants : au moins un membre du secteur de la sécurité en uniforme, au moins un civil et au moins une femme. Par ailleurs, d'autres participants seront invités, provenant des communautés économiques régionales, des organisations multilatérales et du monde universitaire, ainsi que quelques représentants du gouvernement américain.

Les participants doivent être des fonctionnaires de niveau moyen à supérieur, lieutenant-colonel ou équivalent et plus, occupant idéalement des postes responsables de la politique et de la stratégie en matière de cybersécurité ou des technologies émergentes. Voici quelques exemples de nominations possibles :

- Les officiers de l'armée de l'air ou du renseignement militaire qui cherchent à défendre leur pays contre les menaces que représentent les technologies émergentes ;
- Les policiers et les gendarmes des unités de cybermenace ou de renseignement financier chargés de recueillir des preuves numériques ou d'enquêter sur les crimes numériques ; et
- Les fonctionnaires, les personnes nommées ou les experts techniques de haut niveau travaillant sur la cyberpolitique et la stratégie pour les bureaux du président, les ministères des affaires étrangères, les ministères des télécommunications, les conseillers en sécurité nationale et/ou les équipes de réponse aux incidents informatiques (CIRT).

POURQUOI : La pénétration croissante de l'internet et l'innovation rapide en matière de technologie numérique amplifient et modifient la nature des problèmes de sécurité posés par un large éventail d'acteurs étatiques, non étatiques et criminels en Afrique. Le secteur de la sécurité joue un rôle crucial dans la protection des infrastructures nationales essentielles contre les cyberattaques et dans la lutte contre les utilisations malveillantes des technologies de l'information par des acteurs organisés et violents. Une politique efficace en matière de sécurité du cyberspace nécessite une coopération entre toutes les parties concernées.

COMMENT : Cet engagement virtuel combinera des conversations plénières en direct (90 minutes) et des groupes de discussion hebdomadaires, dans le respect de la règle de « non-attribution » (90 minutes). Il sera demandé aux participants de revoir les lectures et les vidéos des cyber-séminaires précédents avant le programme.

Le programme sera composé de quatre séances :

- 1) Le paysage des menaces cybernétiques en Afrique
- 2) Éléments clés d'une réponse nationale en matière de sécurité du cyberspace
- 3) Cybersécurité des infrastructures critiques
- 4) Stratégies de sécurité nationale et de sécurité du cyberspace

Le programme se déroulera en anglais, en français et en portugais.