CENTRE D'ÉTUDES
STRATÉGIQUES DE L'AFRIQUE

Les priorités de la sécurité du cyberespace pour les acteurs de la sécurité nationale en Afrique

PROGRAMME

En ligne, avec Zoom pour le gouvernement

Du 3 au 25 août 2021

CENTRE D'ÉTUDES STRATÉGIQUES DE L'AFRIQUE

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

Du 3 au 25 août 2021

En ligne, Zoom pour le gouvernement

PROGRAMME

SOMMAIRE

À PROPOS DU CENTRE D'ÉTUDES STRATÉGIQUES DE L'AFRIQUE

Depuis sa création en 1999, le Centre d'études stratégiques de l'Afrique a servi de cadre pour la recherche, les formations universitaires et l'échange d'idées ayant pour objectif d'améliorer la sécurité des citoyens en renforçant l'efficacité et la responsabilité des institutions africaines, à l'appui de la politique États-Unis – Afrique.

VISION

La sécurité pour tous les Africains, défendue par des institutions efficaces et responsables envers leurs citoyens.

La concrétisation de la vision d'une Afrique exempte de violence armée organisée, garantie par des institutions africaines engagées dans la protection des citoyens africains, est la motivation principale du Centre d'études stratégiques de l'Afrique. Cet objectif souligne l'engagement du Centre à viser des résultats tangibles, en travaillant avec nos partenaires africains : militaires, civils, gouvernementaux et de la société civile, ainsi que nationaux et régionaux. Tous ont un rôle précieux à jouer dans la réduction des facteurs complexes de conflit existant aujourd'hui sur le continent. La responsabilité envers les citoyens est un élément important de notre vision, car elle souligne le fait que pour être efficaces, les institutions de sécurité doivent non seulement être « fortes », mais également sensibles aux droits des citoyens et les protéger.

MISSION

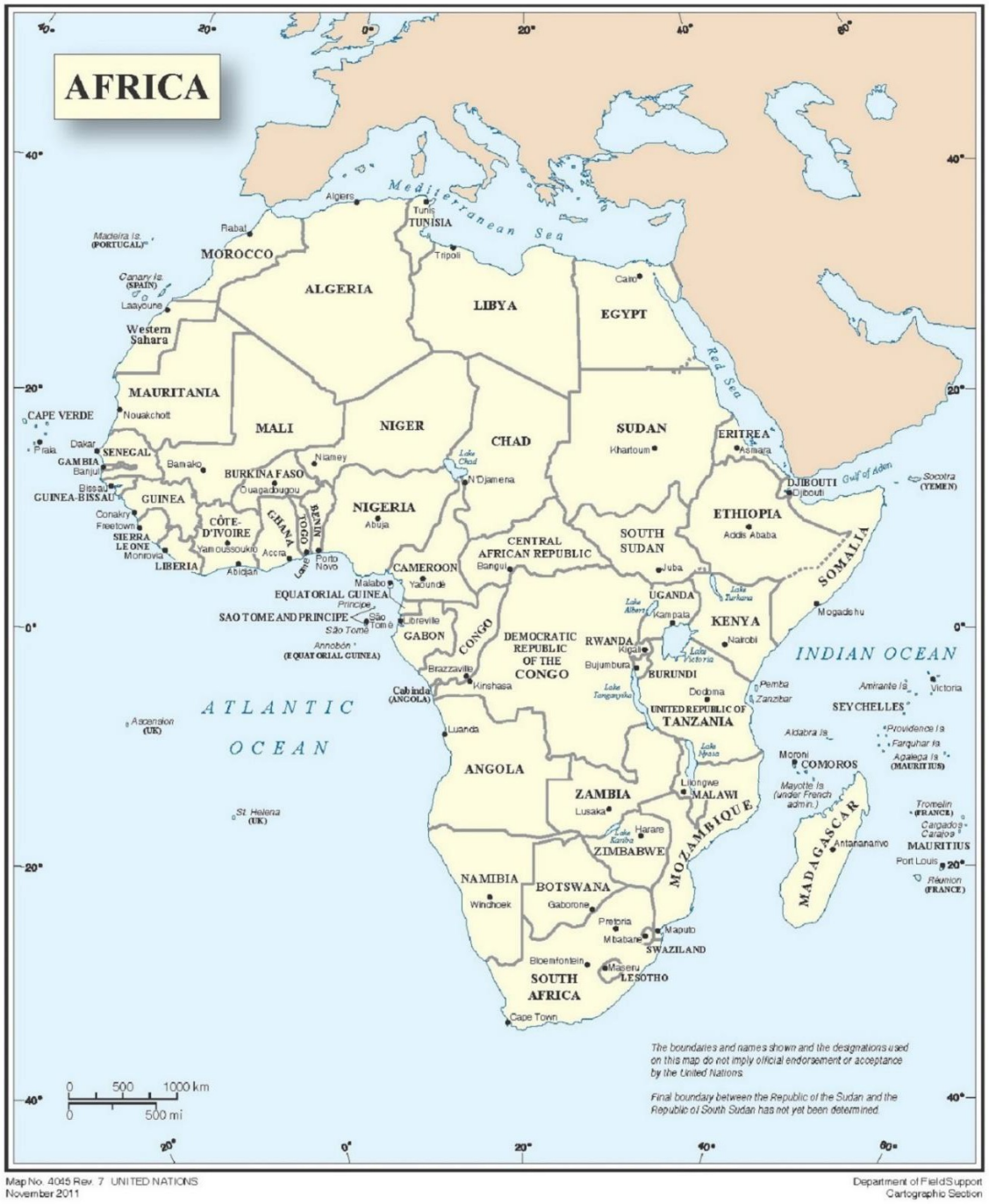
Faire progresser la sécurité africaine en améliorant la compréhension, en fournissant une plate-forme de dialogue fiable, en établissant des partenariats durables et en élaborant des solutions stratégiques.

La mission du Centre d'études stratégiques de l'Afrique tourne autour de la création et de la diffusion des connaissances à travers nos recherches, nos formations universitaires, nos communications stratégiques et nos chapitres communautaires. En nous appuyant sur les expériences pratiques et les leçons tirées des efforts de sécurité sur le continent, nous avons pour objectif de produire des informations et des analyses pertinentes pouvant informer les professionnels et les décideurs des enjeux de sécurité urgents auxquels ils sont confrontés. Nous sommes conscients que relever de sérieux défis ne peut se faire que grâce à des échanges francs et réfléchis. Le Centre fournit des plates-formes en face à face et virtuelles où les partenaires peuvent échanger des points de vue concernant les priorités et les bonnes pratiques. Ces échanges favorisent des relations qui, à leur tour, sont pérennisées grâce aux chapitres communautaires, aux communautés d'intérêts, aux formations de suivi du Centre et au dialogue continu entre les participants et l'équipe. Ce dialogue, imprégné d'expériences du monde réel et d'analyses nouvelles, offre une opportunité d'apprentissage continu et catalyse des actions concrètes.

MANDAT

Le Centre d'études stratégiques de l'Afrique est une institution qui dépend du Département de la Défense des États-Unis, créée et financée par le Congrès pour l'étude des questions de sécurité liées à l'Afrique et servant de cadre pour la recherche bilatérale et multilatérale, la communication, l'échange d'idées et la formation impliquant des participants militaires et civils. *(10 U.S.C 342)*

CARTE DE L'AFRIQUE



Map No. 4045 Rev. 7 UNITED NATIONS
November 2011

Department of Field Support
Cartographic Section

VUE D'ENSEMBLE

L'augmentation du taux d'accès à Internet et les innovations rapides dans le domaine de la technologie numérique sont des facteurs d'amplification de la nature des enjeux de sécurité auxquels l'Afrique est confrontée. Les gouvernements africains, les acteurs du secteur de la sécurité et les citoyens sont vulnérables à une grande diversité de cybermenaces évolutives, de la part de divers acteurs gouvernementaux, non gouvernementaux et criminels. Le cyberespace est devenu le support principal de l'espionnage d'État du fait de la prolifération de capteurs à bas prix, de la technologie de surveillance et de programmes malveillants sophistiqués. La dépendance croissante à la technologie rend vulnérables au cybersabotage les infrastructures essentielles telles que les organisations militaires, les réseaux gouvernementaux et les secteurs tels que ceux de l'énergie et de la banque. De nouvelles formes de criminalité organisée numérique sont en train d'émerger, et des changements sont en cours sur la manière dont les formes plus traditionnelles de criminalité organisée sont organisées et financées. La généralisation des technologies d'information a également des implications sur la manière dont les états violents et les acteurs non gouvernementaux s'organisent, se financent, et sur les stratégies et tactiques qu'ils utilisent pour commettre des violences.

Malgré ces menaces et vulnérabilités croissantes, le secteur de la sécurité africain a été pratiquement absent des efforts nationaux et régionaux destinés à l'amélioration de la sécurité dans le cyberespace. Cependant, le secteur de la sécurité a un rôle crucial à jouer dans la sécurisation des systèmes et des réseaux gouvernementaux, en empêchant la propagation de la cybercriminalité organisée, en protégeant des cyberattaques les infrastructures nationales essentielles, et en offrant une réponse aux autres utilisations malveillantes des technologies de l'information par des intervenants organisés et violents. Pour une politique de sécurité du cyberespace efficace, il est crucial de parvenir à une coopération et une coordination multipartite. Une grande partie de l'innovation, de l'expertise et du capital humain nécessaires à la maturité de la sécurité du cyberespace repose sur le secteur privé. Une supervision exercée par des intervenants civils et par la société civile est nécessaire pour garantir que les politiques de cybersécurité soient bien cohérents avec les principes d'une gouvernance saine du secteur de la sécurité. Afin de garder une longueur d'avance sur les menaces de demain, les gouvernements de l'ensemble du continent devront adapter une approche de la sécurité du cyberespace qui soit collaborative, pangouvernementale et centrée sur les citoyens.

OBJECTIFS DE LA FORMATION :

1. Étendre la compréhension des principaux défis que l'interdépendance de la technologie de l'information pose envers la sécurité de la nation et des citoyens dans les pays africains.

2. Identifier les priorités centrales auxquelles doivent mieux se préparer les acteurs africains de la sécurité et de la défense, et répondre aux cyberactivités malveillantes qui menacent les intérêts de la sécurité nationale.

3. Comparer les expériences, les perspectives et les bonnes pratiques dans le domaine des politiques de sécurité du cyberespace sur divers secteurs : civil, privé et acteurs non gouvernementaux.

4. Partager les avantages à garantir l'accès à un Internet ouvert, fiable et sûr – afin d'optimiser les avantages des technologies d'information interdépendantes pour les entreprises, les gouvernements et les sociétés – tout en réduisant les menaces et les vulnérabilités du cyberespace.

ORGANISATION DE LA FORMATION :

Chaque semaine, la formation comprendra (1) une séance plénière constituée d'un débat modéré avec un ensemble d'experts – des responsables politiques, des professionnels et des universitaires – suivie d'une séance de questions-réponses interactive, et (2) des petits groupes de discussion permettant aux participants de discuter de leurs réactions à la séance plénière et de partager leurs expériences.

La formation se tiendra en anglais, français et portugais. Afin d'encourager des discussions franches et d'établir la confiance entre les participants, une politique de non-attribution sera appliquée, ce qui signifie que les commentaires ou interventions de l'un des participants ne seront identifiés ni par son nom ni par son pays dans les résumés, comptes-rendus ou dans l'échange de connaissances acquises lors du séminaire par tout participant, intervenant ou organisateur.

PROGRAMME :

Ce programme offre une vue d'ensemble des objectifs pédagogiques et des questions stratégiques que cette formation a pour objectif d'aborder au sujet des priorités du secteur de la sécurité africain concernant la sécurité du cyberespace en Afrique. Pour chaque séance, nous offrons une brève introduction et faisons la liste des questions à débattre. Nous incluons également des articles choisis, dont l'objectif premier est d'aider à cerner les enjeux dans le contexte des connaissances disponibles et des documents de politique. Le programme couvre probablement plus de questions et de documentation qu'il ne peut être suffisamment discuté dans le temps disponible. Il est souhaitable de lire une partie ou la totalité des lectures conseillées du programme avant le séminaire, puisque cela placera les participants et les commentaires des intervenants dans le contexte approprié. Cependant, nous espérons également que vous utiliserez ces documents comme ressources même après la fin de la formation, et que vous vous y référerez pour y trouver des détails pertinents.

Les documents externes et le contenu académique inclus dans ce programme ne reflètent pas la vision ou la position officielle du Département de la Défense ou du gouvernement des États-Unis. Ce programme est un document éducatif destiné à présenter diverses opinions et perspectives aux participants, afin de les préparer à profiter au maximum de la formation.

PRÉPARATION DE LA FORMATION :

Avant le séminaire, nous vous encourageons à :

1. Lire ce programme.

2. Lire les lectures conseillées, et regarder les vidéos conseillées.

3. Passer du temps à réfléchir aux questions à débattre et à y répondre.

4. Examiner quelles expériences de votre travail il pourrait être pertinent de partager dans le cadre des groupes de discussion.

5. Vous préparer à participer activement aux groupes de discussion, et à apprendre des participants des autres pays.

Séance plénière 1 : Panorama des cybermenaces de l'Afrique

OBJECTIFS :

- Décrire la portée et l'ampleur des cybermenaces auxquelles les pays africains sont confrontés du fait de l'espionnage, du sabotage des infrastructures critiques, du crime organisé et de la lutte contre l'innovation

- Explorer comment la nature des cybermenaces africaines est susceptible de changer et d'évoluer à l'avenir.

- Considérez la portée et l'ampleur de ces cybermenaces en Afrique du Sud

CONTEXTE :

La diffusion rapide des technologies de l'information et de la communication (TIC) remodèle le panorama de la sécurité en Afrique. Bien que la numérisation ait apporté de nombreux avantages économiques et sociaux, elle amplifie et altère également la nature des enjeux de sécurité du continent. Tous les réseaux informatiques, les réseaux locaux (LAN) et longue distance (WAN) sont vulnérables aux tentatives d'atteinte à la confidentialité, de rupture d'intégrité ou de perturbation de l'accès aux informations qui y sont stockées. Plus largement, l'expansion des TIC modifie comment et par qui les informations sont traitées, enregistrées et diffusées. Ces aspects de la technologie numérique lui permettent d'être exploitée à de sinistres fins par les réseaux criminels, les groupes terroristes, les hackers solitaires, les nations rivales ou tout autre acteur malveillant. Plus le niveau de connectivité est grand, et plus les pays africains et leurs citoyens risquent de voir leurs technologies se retourner contre eux.

Parmi les cybermenaces et enjeux importants pour l'Afrique, on trouve :

- **L'espionnage et la surveillance.** Les systèmes d'information ont fondamentalement transformé les méthodes et les sources que les États-nations, les entreprises et les acteurs non gouvernementaux utilisent pour rassembler et protéger les informations sensibles. Bien que les préoccupations les plus graves liées au cyberespionnage en Afrique soient orientées vers des acteurs étrangers, les capacités d'espionnage et de surveillance se répandent rapidement sur tout le continent.

- **Le sabotage des infrastructures essentielles.** Les réseaux gouvernementaux, les organisations militaires, les industries bancaires et de télécommunications d'Afrique sont vulnérables aux cyberattaques destinées à les incapaciter ou les détruire. Les pays africains sont particulièrement vulnérables du fait que la plus grande partie de l'infrastructure des TIC du continent est fournie par des acteurs extérieurs, et que les secteurs-clés tels que l'électricité, l'eau et l'énergie ont souvent des points de défaillance.

- **La criminalité organisée.** L'expansion du cyberespace a abouti à la formation de formes entièrement nouvelles de réseaux de criminalité organisée, qui exploitent des outils numériques pour voler, transférer et extorquer des ressources. Au cours des dernières années, le continent africain a progressé aussi bien en tant que cible que source de la cybercriminalité organisée. De façon tout aussi importante, la diffusion des TIC influence

également la manière dont les activités criminelles organisées traditionnelles telles que le passage de clandestins, le terrorisme, l'extrémisme violent, la criminalité maritime et le trafic des armes sont structurées et financées.

- **Les innovations liées au combat.** Les technologies de l'information deviennent de plus en plus indispensables à la gestion de la sécurité et à la manière dont elle est assurée auprès des citoyens, y compris les stratégies, les opérations et les tactiques de sécurité. Alors que les institutions et les intervenants de la sécurité de l'ensemble du continent cherchent à profiter des capacités de surveillance accrues et des technologies émergentes telles que les drones, les acteurs non gouvernementaux exploitent les technologies émergentes pour recueillir de l'argent, recruter, organiser et commettre des violences.

QUESTIONS À DÉBATTRE :

- Quels sont les enjeux et les cybermenaces que vous considérez être les plus importants pour votre pays ? Quelle gravité ont-ils ?

- Quels sont les secteurs de votre pays ou région qui sont les plus vulnérables à une cyberattaque ?

- Comment voyez-vous le panorama des cybermenaces évoluer au cours des cinq ou dix ans à venir dans votre pays ?

LECTURES CONSEILLÉES :

Nathaniel Allen, « Africa's Evolving Cyber Threats » (L'Afrique à l'épreuve des nouvelles formes de cybercriminalité), Centre d'études stratégiques de l'Afrique, 2 février 2021.
EN : https://africacenter.org/spotlight/africa-evolving-cyber-threats/
FR : https://africacenter.org/fr/spotlight/lafrique-a-lepreuve-des-nouvelles-formes-de-cybercriminalite/

Noëlle van der Waag-Cowling, « Stepping into the Breach: Military Responses to Global Cyber Insecurity » (S'engouffrer dans la brèche : les ripostes militaires à la cyber insécurité mondiale) Comité International de la Croix-Rouge, 17 juin 2021.
https://blogs.icrc.org/law-and-policy/2021/06/17/military-cyber-insecurity/

Mourad El Manir, « L'Afrique face aux défis proteiformes du cyberespace » Policy Center for the New South, Policy Paper, décembre 2019.
https://www.policycenter.ma/sites/default/files/PP_19-20_Al-Manir.pdf

ENACT et INTERPOL, « *Online Organized African Crime from the Surface to the Darkweb* » (La criminalité organisée africaine du web surfacique au darkweb), Rapport d'analyses INTERPOL, juillet 2020.
https://enact-africa.s3.amazonaws.com/site/ uploads/2020-08-20-interpol-darkweb-report%20.PDF

Union africaine et Symantec, « *Cyber Crime and Cyber Security Trends in Africa* » *(Tendances de la cyber criminalité et de la cyber sécurité en Afrique)*, novembre 2016.

https://thegfce.org/wp-content/uploads/2020/06/CybersecuritytrendsreportAfrica-en-2.pdf

VIDÉOS CONSEILLÉES :

Centre d'études stratégiques de l'Afrique, « Emerging Cyber Dimensions of Africa's Security Landscape » (Les nouvelles cyber-dimensions du paysage sécuritaire africain), 3 décembre 2020
EN : https://africacenter.org/programs/emerging-cyber-dimensions-africa-security- landscape/
FR : https://africacenter.org/fr/programs/nouvelles-cyber-dimensions-paysage-securitaire-africain/
PO : https://africacenter.org/pt-pt/dimensoes-ciberneticas-emergentes-paisagem-seguranca-africa/

Centre d'études stratégiques de l'Afrique, « Cyber Dimensions of Violent Extremism in Africa » (Les dimensions cybernétiques de l'habileté politique en Afrique), 18 mars 2021
EN : https://africacenter.org/programs/cyber-dimensions-statecraft-africa/
FR : https://africacenter.org/fr/programs/dimensions-cybernetiques-habilete-politique-afrique/
PO : https://africacenter.org/pt-pt/dimensoes-ciberneticas-aparelho-estado-africa/

Centre d'études stratégiques de l'Afrique, « Cyber Dimensions of Violent Extremism in Africa » (Les dimensions cybernétiques de l'extrémisme violent en Afrique), 19 mai 2021
EN : https://africacenter.org/programs/cyber-violent-extremism-africa/
FR : https://africacenter.org/fr/programs/dimensions-cybernetiques-extremisme-violent-afrique/
PO : https://africacenter.org/pt-pt/dimensoes-ciberneticas-extremismo-violento-africa/

Centre d'études stratégiques de l'Afrique, « Emerging Cyber Dimensions of Transnational Organized Crime in Africa » (Les dimensions cybernétiques de la criminalité transnationale organisée en Afrique), 8 juillet 2021
EN: https://africacenter.org/programs/cyber-dimensions-of-organized-crime-in-africa/
FR : https://africacenter.org/fr/programs/les-dimensions-cybernetiques-de-la-criminalite-organisee-en-afrique/
PO: https://africacenter.org/pt-pt/dimensoes-ciberneticas-do-crime-organizado-em-africa/

Séance plénière 2 : Principaux éléments d'une riposte nationale sécuritaire dans le cyberespace

OBJECTIFS :

- Identifier les éléments principaux d'une riposte au niveau national nécessaires pour affronter les enjeux à la sécurité nationale relatifs au cyberespace.

- Identifier les intervenants et les acteurs principaux permettant de concevoir et de mettre en œuvre une riposte de sécurité nationale dans le cyberespace, et le rôle des acteurs de la sécurité nationale dans le cadre d'une approche multipartite.

- Évaluer les politiques, les stratégies et les institutions de sécurité au niveau national, relatives au cyberespace dans de grands pays africains.

- Faire le point du rôle du secteur de la sécurité dans le cadre de la démarche nationale de confrontation des cybermenaces en relation avec l'espionnage, le sabotage des infrastructures essentielles, la criminalité et l'innovation liée au combat.

- Débattre des avantages et des enjeux liés à l'accès à un Internet ouvert, fiable et sûr – afin d'optimiser les avantages des technologies d'information interdépendantes pour les entreprises, les gouvernements et les sociétés – tout en réduisant les menaces et les vulnérabilités du cyberespace.

CONTEXTE :

La stratégie et la politique de cybersécurité sont encore balbutiantes dans une grande partie de l'Afrique. La plupart des pays africains ne disposent ni de stratégies de cybersécurité, ni d'équipes nationales d'intervention en cas d'incident de sécurité informatique, ce qui est le strict minimum pour une infrastructure nationale de gestion des cybermenaces. Dans les plus grands pays, le rôle du secteur de la sécurité dans le cadre plus large de la riposte de cybersécurité est très variable. Au Kenya, au Sénégal et à Maurice, les ministères des télécommunications sont les organismes principaux ayant la responsabilité de superviser la politique de cybersécurité. Au Nigeria et en Afrique du Sud, le secteur de la sécurité a pris une plus grande place : les principaux intervenants sont respectivement le Conseiller pour la sécurité nationale et l'Agence de sécurité de l'État.[1]

Confronter les cyber menaces évolutives du continent exige une riposte complète et supervisée par le gouvernement. Parmi les principaux éléments de cette riposte, on trouve : [2]

a) Les stratégies nationales, qui structurent la vision de la cybersécurité et les objectifs stratégiques, qui identifient et priorisent les enjeux de cybersécurité les plus essentiels

[1] Un recueil des stratégies nationales de cybersécurité de chaque pays se trouve sur le site Internet de L'Union Internationale des Télécommunications à l'adresse https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.

[2] Pour une structure internationalement acceptée, consultez par exemple l'Oxford Cyber Maturity Model (schéma de cybermaturité d'Oxford) : https://gcscc.ox.ac.uk/cmm-dimensions-and-factors#collapse2008981

d'un pays, affectent les ressources, attribuent les responsabilités de cybersécurité au sein du gouvernement, et garantissent une supervision civile des acteurs de la sécurité.

b) Les structures légales et réglementaires, qui abordent la croissance de la cybercriminalité organisée et encouragent la capacité des forces de l'ordre à utiliser des preuves numériques.

c) Les équipes d'intervention et de gestion de crise en cas d'incident de sécurité informatique, qui peuvent identifier, surveiller et protéger les infrastructures nationales essentielles de l'information, et contribuer au rétablissement de la situation après les inévitables failles de sécurité.

d) La cybersensibilisation du secteur de la sécurité nationale, l'identification des menaces et la capacité de riposte.

Quels que soient le pays ou le contexte, une coordination multipartite est indispensable pour une riposte nationale efficace. Le secteur privé, la société civile et les acteurs de la sécurité sont des partenaires importants, et non des opposants ou des obstacles, pour les acteurs gouvernementaux et du secteur de la sécurité qui cherchent à développer des approches nationales saines de sécurité du cyberespace. Les gouvernements de toute l'Afrique comptent sur le secteur privé pour fournir la toute dernière technologie de cybersécurité, pour signaler les incidents et surveiller les menaces, et pour occuper un rôle de premier plan dans la sécurisation des secteurs-clés contre les cyberattaques – tels que les télécommunications et les banques. La société civile est un partenaire tout aussi essentiel qui permet de garantir que la politique de cybersécurité reste conforme avec les droits humains, la démocratie et la sécurité des citoyens. Le succès d'organisations telles que le Kenya ICT Action Network[3] pour favoriser le dialogue public et catalyser le secteur des TIC souligne l'importance d'une approche multipartite dans le domaine de la sécurité du cyberespace.

Ce qui importe le plus est la manière dont la politique et la stratégie de cybersécurité sont formulées et mises en œuvre. Une trop faible implication du secteur de la sécurité peut amener un pays à échouer à sécuriser les réseaux sensibles du gouvernement, à développer la capacité de surveillance, à riposter à la criminalité organisée et à intégrer la technologie numérique dans les stratégies, les opérations et les tactiques militaires. Cependant, une trop forte présence du secteur de la sécurité peut engendrer des coûts superflus et réduire la supervision civile ainsi que la responsabilité. Quel que soit leur rôle, il est essentiel que les acteurs gouvernementaux et du secteur de la sécurité gardent à l'esprit que la sécurité des citoyens est indispensable à la cybersécurité. Ils doivent guider les efforts de riposte aux menaces posées par la diffusion de la technologie numérique, d'une manière compatible avec les valeurs consacrées par l'Architecture africaine de paix et de sécurité : état de droit, droits humains et démocratie.

QUESTIONS À DÉBATTRE :

- Quelle est l'efficacité de votre pays/région dans la riposte aux cybermenaces, et quels sont les enjeux ?

[3] Pour plus d'informations sur le Kenya ICT Action Network, consultez : https://www.kictanet.or.ke/about-kictanet/

- Quel est dans votre pays le rôle que joue le secteur de la sécurité dans la sécurité du cyberespace ? Quels autres intervenants sont impliqués dans la sécurité du cyberespace dans votre pays ?

- Quel est le rôle que doit avoir le secteur de la sécurité pour faire face aux cybermenaces et aux enjeux qui affectent votre pays ? Comment cela pourrait-il accompagner une approche multipartite ?

- Quels sont les enjeux et les risques associés à l'implication du secteur de la sécurité dans la sécurité du cyberespace ?

LECTURES CONSEILLÉES :

Global Cyber Security Capacity Centre, « Cyber Maturity Model Dimension 1: Cybersecurity Policy and Strategy » (Modèle de cyber maturité dimension 1 : politique et stratégie de la cybersécurité), Oxford University.
https://gcscc.ox.ac.uk/cmm-dimensions-and-factors#collapse2008981

Global Forum on Cyber Expertise, « Delhi Communiqué on a GFCE Agenda for Global Cyber Capacity Building » (Communiqué de Delhi sur un calendrier du GFCE sur le renforcement des cybercapacités mondiales), 24 novembre 2017.
https://thegfce.org/wp-content/uploads/2020/04/ DelhiCommunique.pdf

Union internationale des télécommunications des Nations Unies, « 2020 Global Cybersecurity Index » (Répertoire mondial 2020 de la cybersécurité) Nations Unies, 29 juin 2021.
https://www.itu.int/en/myitu/Publications/2021/06/28/13/22/Global-Cybersecurity-Index-2020

DCAF, « How do Cyberspace and Cybersecurity Relate to Good Security Sector Governance » (Quel rapports le cyberespace et la cybersécurité entretiennent-ils avec une bonne gouvernance du secteur de la sécurité) dans *Guide to Good Governance in Cybersecurity,"* p. 25 à 38, janvier 2021.
EN : https://www.dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_ENG_Jan2021_0.pdf#page=25
FR : https://www.dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_Jan2020.pdf

« A Problemática Da Cibersegurança E Os Seus Desafios » (La question de la cybersécurité et ses défis), Centro de I&D Sobre direito e sociedade, septembre 2016.
http://cedis.fd.unl.pt/wp-content/uploads/2017/10/CEDIS-working-paper_DSD_A-problemática-da-cibersegurança-e-os-seus-desafios.pdf

Nathaniel Allen, « The Promises and Perils of Africa's Digital Revolution » (Les promesses et les périls de la révolution numérique de l'Afrique), Brookings Techstream Blog, 11 mars 2021.
https://www.brookings.edu/techstream/the-promises-and-perils-of-africas-digital-revolution/

Séance plénière 3 : Gestion des cyberincidents et protection des infrastructures essentielles

OBJECTIFS :

- Définir les infrastructures essentielles et examiner l'échelle et la portée des menaces liées au cyberespace et à ses vulnérabilités dans les pays africains.

- Discuter du rôle des équipes nationales et sectorielles d'intervention en cas d'incident de sécurité informatique (CSIRT) dans le cadre d'un système national de riposte de cybersécurité, qui permet d'identifier et de réagir aux cyberattaques malveillantes sur les infrastructures essentielles.

- Discuter du rôle que les acteurs de la sécurité nationale jouent en tant que membres des CSIRT, des cellules de coordination interagences et des autres mécanismes de coopération interagences pour la sécurité du cyberespace.

- Étudier quelle est la meilleure façon de promouvoir des partenariats transversaux entre les acteurs civils et le secteur de la sécurité, les forces de l'ordre, la justice et les partenaires du secteur privé, dans le but de sécuriser les infrastructures essentielles tributaires d'Internet.

CONTEXTE :

Alors que les pays africains se développent et se numérisent, leurs systèmes d'infrastructures essentielles (CI) de services et d'actifs sont de plus en plus vulnérables aux cyberattaques. L'Union Internationale des Télécommunications (UIT) propose une définition de principe des infrastructures essentielles comme étant « des systèmes, services ou fonctions de base dont l'interruption ou la destruction aurait un impact incapacitant sur la santé et la sécurité publiques, le commerce, la sécurité nationale ou toute association de ceux-ci. »[4] Les infrastructures essentielles de l'information (CII) sont une composante des infrastructures essentielles, tout comme les TIC, qui sont nécessaires pour le fonctionnement complet de multiples secteurs des dites infrastructures essentielles.[5] Les ressources des infrastructures essentielles de l'information fonctionnent au sein d'un réseau de secteurs interconnectés et interdépendants où leurs systèmes sont affectés de vulnérabilités intrinsèques, qui pourraient être exploitées en attaquant les systèmes de contrôle de l'une des ressources de l'infrastructure. Des attaques visant ces « systèmes de contrôle », y compris le contrôle des données de régulation et les systèmes de contrôle et d'acquisition de données (SCADA) et de commandement des interventions (ICS) peuvent produire des dommages dans d'autres infrastructures essentielles par effet domino.

La cybersécurité des infrastructures essentielles implique des efforts soutenus afin de sécuriser celles-ci des attaques extérieures, ainsi qu'une volonté durable de préserver la continuité des

[4] Groupe d'étude UIT question 22/1 « Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts » (Rapport sur les meilleures pratiques d'une approche nationale de la cybersécurité : un cadre de gestion de l'organisation des efforts nationaux de cybersécurité), Secrétariat de l'ITU-D, Genève (2008).
[5] Maglaras, Leandros, et al. « Threats, countermeasures and attribution of cyber attacks on critical infrastructures. » (Menaces, contre-mesures et attribution des cyberattaques sur les infrastructures essentielles). EAI Endorsed Transactions on Security and Safety 5.16 (2018).

services d'infrastructure lorsque des incidents mettant en cause la sécurité informatique se produisent. Les équipes d'intervention en cas d'incident de sécurité informatique (CSIRT) font partie intégrante du système de protection des infrastructures d'information essentielles, offrant une gestion de riposte en cas d'incidents ou d'urgences, surveillant l'environnement des menaces, ripostant et permettant une récupération en cas de cyberattaque importante. Au niveau national, les CSIRT offrent des services vastes et étendus au pays, en travaillant en étroite collaboration avec les CSIRT sectoriels et privés, ce qui permet un échange d'informations et de communications pertinentes et ponctuelles.

Les pays africains font face à des occasions mais aussi à des entraves lorsqu'il s'agit de protéger leurs infrastructures essentielles des cyberattaques. D'un côté, un niveau limité de dépendance aux technologies par rapport aux régions du monde qui sont plus industrialisées, ainsi que des systèmes anciens, donnent à de nombreuses nations africaines la possibilité d'intégrer la cybersécurité dès la création de leurs réseaux infrastructurels. D'un autre côté, une grande dépendance aux acteurs extérieurs dans la fourniture des infrastructures essentielles, des points de défaillance et des investissements limités dans la cybersécurité des infrastructures essentielles posent des risques notables. Seuls 22 pays d'Afrique disposent de CSIRT nationaux, [6]en partie du fait qu'ils exigent un investissement énorme en temps, en argent et en ressources techniques. [7] L'existence de CSIRT au niveau sectoriel est rare, en partie du fait de la présence d'entreprises et d'organisations petites et moyennes qui elles-mêmes font face à des contraintes de ressources similaires.

QUESTIONS À DÉBATTRE :

- Que décririez-vous comme une infrastructure essentielle dans votre pays ou votre région ? Dans quelle mesure cette infrastructure essentielle est-elle cyberdépendante ?

- Est-ce que votre pays dispose de CSIRT et quelle est leur efficacité pour protéger l'infrastructure cybernétique essentielle ?

- Quels sont les mécanismes, les lois ou les politiques mis en place dans votre pays pour protéger les infrastructures essentielles nationales des cyberattaques ?

- Quel est le rôle du secteur de la sécurité dans la protection des infrastructures essentielles nationales dans votre pays ?

- Comment la coopération, la coordination et le partage d'informations entre le secteur de la sécurité, les autres parties du gouvernement et des intervenants non gouvernementaux peuvent-ils être améliorés afin d'augmenter la résilience des infrastructures nationales cyberdépendantes ?

LECTURES CONSEILLÉES :

[6] Consultez les toutes dernières données de l'Union internationale des télécommunications : https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

[7] Jean Mouton et Ian Ellefsen. « The identification of information sources to aid with critical information infrastructure protection » (L'identification des sources d'information contribue à la protection des infrastructures essentielles de l'information). 2013 Information Security for South Africa (2013) : 1 à 8.

Nathaniel Allen et Noelle van der Waag-Cowling, « How African Countries Should Address State-Sponsored Cyber Threats » (Comment les pays africains devraient aborder les menaces cybernétiques des états) Brookings Techstream Blog, 15 juillet, 2021 https://www.brookings.edu/techstream/how-african-states-can-tackle-state-backed-cyber-threats/

Internet Society et Commission de l'Union africaine, « Lignes directrices sur la sécurité de l'infrastructure Internet pour l'Afrique », 24 mai 2017.
EN : https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa
FR : https://www.internetsociety.org/fr/resources/doc/2017/lignes-directrices-sur-la-securite-de-linfrastructure-internet-pour-lafrique

Redação Digital Security, « La cybersécurité doit être une priorité pour le secteur des infrastructures critiques », 28 septembre 2020.
https://revistadigitalsecurity.com.br/seguranca-cibernetica-deve-ser-prioridade-para-setor-de-infraestrutura-critica/

Hanneke Duijnhoven, Bram Poppink, Tom van Schie et Don Stikvoort, « Getting Started with a National Computer Security Incident Response Team (CSIRT) Guide » (Démarrer avec une équipe d'intervention en cas d'incident de sécurité informatique [CSIRT]), Nederlandse Organisatie voor Wetenschappelijk Onderzoek (Organisation néerlandaise pour la recherche scientifique), 2021.
https://cybilportal.org/tools/getting-started-with-a-national-csirt-guide/

Eric Luiijf, Tom van Schie, Theo van Ruijven et Auke Huistra, « The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers » (Le guide des bonnes pratiques de GFCE-MERIDIAN sur la protection des infrastructures essentielles de l'information pour les décideurs politiques gouvernementaux), GFCE-Meridian, 2016. https://www.tno.nl/media/8578/gpg_criticalinformationinfrastructureprotection.pdf

Séance plénière 4 : Stratégie nationale de cybersécurité

OBJECTIFS :

- Discuter du processus de rédaction d'une stratégie nationale de sécurité du cyberespace, et identifier ses éléments fondamentaux.

- Discuter du rôle des acteurs du secteur de la sécurité dans la conception et la mise en œuvre d'une stratégie et d'une politique nationale de cybersécurité.

- Souligner les principes fondamentaux, les bonnes pratiques et les leçons apprises au cours de la conception et de la mise en œuvre de la stratégie et de la politique nationale de cybersécurité.

CONTEXTE :

Sur de nombreux plans, les stratégies de cybersécurité sont au cœur des efforts nationaux visant à riposter aux cyberdéfis. Les stratégies nationales de cybersécurité sont nécessaires afin de définir et de prioriser les principales menaces, lesquelles varient de façon significative d'un pays à l'autre et d'une région à l'autre. La législation et les stratégies nationales sont les vecteurs principaux permettant de distribuer les rôles et les responsabilités concernant la sécurité du cyberespace au niveau intergouvernemental. Elles peuvent également être utilisées comme outils permettant de garantir que la cybersécurité dispose des ressources adéquates, et pour surveiller les progrès de la défense contre les cybermenaces au niveau national. Si elles sont régulièrement mises à jour, les stratégies de cybersécurité peuvent garantir que les efforts de sécurité liés au cyberespace répondent et s'adaptent à un environnement évolutif des menaces.

Comme pour toute stratégie liée à la sécurité, le processus par lequel la stratégie est élaborée est aussi important que son contenu. L'adhésion et le soutien à un haut niveau politique sont nécessaires pour résoudre les conflits pouvant survenir entre différents organismes et ministères, ainsi que pour garantir une communication claire et cohérente avec le public. Avec un processus clair de priorisation des menaces, les stratégies nationales peuvent constituer des outils utiles pour gérer de maigres ressources gouvernementales et diriger les soutiens externes vers les points où ils sont le plus nécessaires. Les stratégies qui résultent d'une consultation avec une grande variété d'intervenants gouvernementaux, de la société civile et externes peut parvenir à une large adhésion, à améliorer la coordination du gouvernement et à catalyser les efforts nationaux visant à aborder les principaux enjeux de sécurité.[8] Ces considérations sont particulièrement essentielles dans le contexte africain, où les gouvernements se reposent souvent sur le soutien d'intervenants extérieurs, et où une implication multipartite est indispensable pour garantir la responsabilité, l'inclusion et le respect de la sécurité des citoyens.

Malheureusement, la plupart des gouvernements africains n'ont pas encore élaboré de stratégie nationale de cybersécurité. Suivant les données les plus récentes communiquées par l'Union internationale des télécommunications des Nations Unies, seuls 16 pays d'Afrique sur 54 sont des

[8] Consultez le Centre d'études stratégiques de l'Afrique, « Boîte à outils de l'élaboration de la stratégie de sécurité nationale » 2021. https://africacenter.org/wp-content/uploads/2021/01/Developpement-dune-strategie-de-securite-nationale-en-Afrique-outil-de-consultation-et-de-redaction-CESA.pdf

stratégies nationales de cybersécurité abouties. Les stratégies de quatre pays supplémentaires – la Tunisie, le Botswana, le Ghana et la Zambie – sont encore à l'état d'ébauches.[9] Même dans les pays où la pénétration d'Internet est faible, le manque d'une stratégie nationale de cybersécurité est une occasion manquée d'optimiser les bénéfices et de réduire les risques liés à une numérisation croissante.

QUESTIONS À DÉBATTRE :

- Pour les pays disposant d'une stratégie nationale de cybersécurité, quel processus avez-vous suivi pour le développement ou la mise en œuvre de la stratégie de votre pays ? Pour les pays ne disposant pas d'une stratégie nationale de cybersécurité déjà en place, quelle a été votre expérience concernant la conception et la mise en œuvre de stratégies sectorielles et de politiques sur les questions de cybernétique ?

- Quel rôle le secteur de la sécurité a-t-il ou devrait-il avoir dans le processus de conception d'une stratégie de sécurité du cyberespace ?

- Quelles sont les bonnes pratiques, procédures, mécanismes de coordination ou de surveillance qui sont nécessaires pour garantir que les acteurs de la sécurité nationale jouent un rôle productif dans l'élaboration des politiques et des stratégies sur les questions relatives à la cybernétique ?

LECTURES CONSEILLÉES :

Union Internationale des Télécommunications (UIT), « *Guide pour l'élaboration d'une stratégie nationale de cybersécurité* », 2018.
EN : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf
FR : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-F.pdf

Centre d'études stratégiques de l'Afrique, « Développement d'une stratégie de sécurité nationale en Afrique », section 1, pages 1 à 9, 2021.
EN : https://africacenter.org/wp-content/uploads/2021/01/National-Security-Strategy-Development-in-Africa-Toolkit-for-Drafting-and-Consultation-Africa-Center-for-Strategic-Studies.pdf
FR : https://africacenter.org/wp-content/uploads/2021/01/Developpement-dune-strategie-de-securite-nationale-en-Afrique-outil-de-consultation-et-de-redaction-CESA.pdf
PO : https://africacenter.org/wp-content/uploads/2021/02/Desenvolvimento-da-Estrategias-de-Seguranca-Nacional-em-Africa-Um-kit-de-ferramentas-para-consulta-e-preparacao.pdf

Luka Kuol et Joel Amegboh, « Rethinking National Security Strategies in Africa » (Repenser les stratégies de sécurité nationales en Afrique) *International Relations and Diplomacy* 9 (01) : 2021, 1 à 17. http://www.davidpublisher.org/Public/uploads/Contribute/60a72058556ba.pdf

Gouvernement du Burkina Faso, « Stratégie nationale de cybersécurité » janvier 2019.
https://anssi.bf/fileadmin/user_upload/SNCS_BF.pdf

[9] Voir le recueil des stratégies nationales de cybersécurité de l'Union Internationale des Télécommunications (UIT) : https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

République fédérale du Nigeria, « *National Cybersecurity Strategy and Policy* » *(Stratégie et politique nationale de cybersécurité)*, février 2021. https://www.cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf

Claudia Almeida et al., « Problemática da Cibersegurança: o Caso da Estratégia Nacional de Segurança no Ciberespaço » (Problématique de cybersécurité : le cas de la stratégie nationale de sécurité du cyberespace) *Informação e Segurança no Ciberespaço*, septembre 2018. https://www.researchgate.net/publication/327515395_A_Problematica_da_Ciberseguranca_o_Caso_da_Estrategia_Nacional_de_Seguranca_no_Ciberespaco