AFRICA CENTER
FOR STRATEGIC STUDIES

PRIORITÉS EN MATIÈRE DE SÉCURITÉ DU CYBERESPACE POUR LES ACTEURS DE LA SÉCURITÉ NATIONALE EN AFRIQUE
PROGRAMME D'ÉTUDES VIRTUEL

DOCUMENT DE SYNTHÈSE

Du 3 au 25 août 2021

Du 3 au 25 août 2021, le Centre d'études stratégiques de l'Afrique a organisé un programme en ligne de niveau exécutif sur le rôle du secteur de la sécurité dans la résolution des défis et menaces liés à la cybernétique en Afrique. Ce document de synthèse présente le contexte, synthétise les perspectives des participants, partage les idées clés et identifie les tendances émergentes discutées au cours du programme. Les réflexions portent sur la manière dont les acteurs de l'État, du secteur de la sécurité, du secteur privé et de la société civile en Afrique peuvent :

- Améliorer la connaissance des menaces et des acteurs les plus importants dans le domaine de la cybercriminalité.
- Mettre en œuvre des approches multipartites de la cybersécurité
- Exploiter les avantages et limiter les risques de la participation du secteur de la sécurité à la cybersécurité
- Aligner la politique et la stratégie de cybersécurité sur les droits humains et le respect de l'État de droit

Contexte

Le séminaire a réuni des participants représentant 30 pays africains, issus du monde civil et militaire, ainsi que des représentants du secteur privé, de la société civile et des organisations régionales. Les objectifs des participants étaient les suivants : i) mieux comprendre les menaces et les défis liés à la cybercriminalité en Afrique, ii) identifier les principales priorités des acteurs de la sécurité nationale et de la défense pour répondre aux cyberactivités malveillantes, et iii) discuter de la manière de maximiser les avantages des technologies de l'information tout en minimisant les menaces et les vulnérabilités en matière de cybersécurité.

La réunion de participants venant d'horizons divers et de milieux civils et militaires a permis un dialogue holistique, respectueux et éclairé sur le rôle du secteur de la sécurité dans la cybersécurité en Afrique. La première partie du programme s'est attachée à comprendre le paysage des cybermenaces en Afrique dans une perspective de sécurité nationale. Les autres séances ont porté sur les éléments clés d'une réponse nationale en matière de cybersécurité, en se concentrant spécifiquement sur la réponse aux incidents de sécurité informatique, la protection des infrastructures critiques et la mise en œuvre de stratégies nationales de cybersécurité.

Le point de vue des participants sur le défi

Les participants ont discuté de la manière dont la diffusion rapide des technologies de l'information rend leurs pays vulnérables aux menaces que représentent le cyberespionnage, le sabotage des infrastructures critiques, la criminalité organisée et la lutte contre l'innovation. Ils ont discuté de la façon dont les acteurs les plus importants en matière de menaces ont historiquement été les acteurs criminels étatiques et transnationaux extérieurs à l'Afrique, mais qu'il y a une inquiétude croissante quant à la propagation rapide des cybermenaces stratégiques à l'intérieur du continent. Dans un sondage réalisé au cours de la première séance plénière, les participants ont classé les réseaux criminels organisés et l'extrémisme violent comme les acteurs de la cybermenace qui les préoccupent le plus, ce qui correspond étroitement aux préoccupations traditionnelles des responsables africains en matière de sécurité concernant ces acteurs.

En outre, les participants ont souligné l'importance de la nécessité d'adopter une optique de sécurité centrée sur le citoyen dans la gestion des cybermenaces et des défis. En raison de la nature interne de la plupart des conflits en Afrique, le contrôle et l'accès à la population comptent souvent autant que la violence physique. Étant donné que les technologies de l'information jouent un rôle de plus en plus central dans la manière dont les États informent, accèdent et fournissent des services à leurs populations, les gouvernements devraient utiliser ces technologies non seulement pour lutter directement contre les menaces et les vulnérabilités, mais aussi pour renforcer le contrat social entre les gouvernements et les citoyens.

Comment les gouvernements africains peuvent-ils trouver un équilibre entre la nécessité d'impliquer le secteur de la sécurité dans le cyberespace tout en limitant les risques et en renforçant le contrat social ? Les participants ont proposé quatre idées clés.

Informations clés

1. **Les acteurs du gouvernement, du secteur de la sécurité, de la communauté internationale et du secteur privé devraient travailler ensemble pour améliorer la sensibilisation aux menaces et aux acteurs les plus importants de la cybercriminalité.** Pratiquement tous les États africains disposent désormais, au minimum, d'une cyberunité chargée de surveiller et de combattre la cybercriminalité. Toutefois, la connaissance de la manière dont les acteurs les plus déstabilisants, tels que les réseaux criminels organisés, les groupes extrémistes violents et les États-nations, exploitent le cyberespace et à quelles fins est plus limitée. Même les pays africains plus matures sur le plan cybernétique n'en sont encore qu'au stade initial de la détermination du rôle éventuel que les technologies de l'information doivent jouer dans la manière dont le secteur de la sécurité surveille ces menaces et y répond, ainsi que du rôle du secteur de la défense dans le cadre d'une réponse nationale plus large en matière de cybersécurité. Les participants ont suggéré que la sensibilisation aux menaces et défis cybernétiques les plus importants du continent pourrait être améliorée par les moyens suivants :

    - *La cyber-sensibilisation de base et le renforcement des capacités dans les pays moins matures sur le plan cybernétique*. Les pays africains les moins matures sur le plan cybernétique devraient commencer par une formation de base à la cyberconscience et au renforcement des capacités. Le renforcement des capacités devrait « être le fondement de la transformation numérique et être adapté à l'importance de la menace. » Dans les pays où de larges pans de la population n'ont pas accès à l'internet, ces efforts devront être menés en tandem avec ceux

visant à améliorer la pénétration de l'internet et la culture numérique de base. Pour les personnes disposant d'un accès à l'internet, les participants ont conseillé d'explorer les moyens de sensibiliser et de renforcer les capacités à peu ou pas de frais, grâce à de nombreux cours et formations en ligne gratuits.

- *Une surveillance et un signalement plus concertés des menaces dans les pays plus matures sur le plan cybernétique*. Pour les pays qui en ont la capacité, les participants ont suggéré que davantage d'efforts étaient nécessaires pour surveiller, suivre et rendre compte des menaces. Peu de pays, par exemple, publient régulièrement des informations sur le type et le volume des attaques informatiques qu'ils subissent ou surveillent les activités en ligne des acteurs de la menace les plus importants et les plus déstabilisants. Souvent, ce sont des tiers qui identifient et informent les parties concernées d'une violation. Cela s'explique en partie par le fait que la cybersécurité est considérée comme une question sensible et que tant les gouvernements que le secteur privé sont réticents à signaler ou à divulguer les attaques. En sensibilisant l'ensemble du continent au paysage des cybermenaces, les participants ont suggéré qu'une transparence et une collaboration bien plus grandes étaient nécessaires pour instaurer la confiance entre les multiples groupes de parties prenantes, afin de leur permettre de surveiller, de dissuader et de prévenir les cyberactivités malveillantes.

2. **Les réponses aux menaces et défis cybernétiques, même les plus importants, doivent s'appuyer sur une approche multipartite.** Contrairement à d'autres technologies qui sont explicitement conçues pour causer des dommages physiques, les technologies de l'information ont un large éventail d'utilisations, dont beaucoup, si ce n'est la plupart, visent à tirer des avantages économiques et sociaux. Le capital humain, l'expertise technique et les capacités de défense du secteur privé, notamment dans les secteurs de la finance et de la technologie, dépassent généralement ceux des acteurs gouvernementaux. En outre, les technologies de l'information devenant de plus en plus essentielles à la manière dont les gouvernements servent leurs citoyens, les parties prenantes de l'industrie privée et de la société civile ont un rôle essentiel à jouer dans le choix de l'utilisation des technologies de l'information. Il a été noté que la culture de la cyberdéfense en Afrique doit changer, notamment parce que, dans de nombreux cas, les civils sont plus compétents que les acteurs du secteur de la sécurité en termes de cyberconscience et de niveau de formation. Les participants ont souligné que les ingrédients essentiels à la conception et à la mise en œuvre réussies d'une stratégie et d'une politique multipartites en matière de cybersécurité étaient les suivants :

   - *Inclusivité et confiance*. La conception et la mise en œuvre de la stratégie, de la législation et de la politique nationales en matière de cybersécurité doivent viser à inclure et à intégrer le retour d'information de « toutes les parties prenantes concernées » dans la conception, la rédaction et la mise en œuvre. Il s'agit, au minimum, du secteur de la sécurité, des télécommunications, de la finance, de l'énergie, de la société civile, du monde universitaire et d'autres secteurs jugés essentiels pour la protection des infrastructures critiques cyberdépendantes. Les participants ont noté que l'inclusion contribue à renforcer la confiance du public dans les cyberautorités nationales en permettant la coopération entre plusieurs parties prenantes et le signalement des incidents. Sans cette confiance du public, les efforts déployés pour contrer les cybermenaces seront moins fructueux.

   - *Un leadership politique de haut niveau.* En raison de la diversité des parties prenantes, les processus stratégiques et politiques en matière de cybersécurité ne sont généralement pas

efficaces sans un leadership politique de haut niveau permettant de répartir les rôles et les responsabilités et d'arbitrer les différends entre les agences. Au Ghana, ce rôle a été assumé par un groupe de travail interministériel. Au Nigeria et au Burkina Faso, cette responsabilité incombait respectivement au conseiller à la sécurité nationale et à l'Agence nationale de sécurité des systèmes d'information (ANSSI), deux entités extra-ministérielles qui dépendent directement du président.

- *Tirer parti de l'expertise technique.* La conception et la mise en œuvre des stratégies et politiques nationales en matière de cybersécurité doivent s'appuyer sur une expertise technique. Au Niger, l'Agence nationale pour la société de l'information joue un rôle clé dans l'élaboration d'une stratégie nationale de cybersécurité et accueillera à terme l'équipe nationale de réponse aux incidents de sécurité informatique (CSIRT). Au Ghana, ce rôle est joué par un groupe de travail technique chargé de mettre en œuvre les cyberpolitiques nationales et de faire des recommandations au comité interministériel. La CSIRT nationale du Ghana a également joué un rôle important dans la mise en place et la coordination des efforts des CSIRT régionales et sectorielles, qui restent rares en Afrique.

3. **Le secteur de la sécurité a un rôle crucial à jouer dans la sécurité du cyberespace, mais un rôle qui comporte à la fois des risques et des avantages.** Tout en reconnaissant qu'il n'existe pas d'approche unique**,** les participants s'accordent à dire que le secteur de la sécurité en Afrique a un rôle essentiel à jouer dans le cadre d'une réponse nationale plus large en matière de cybersécurité. Les participants ont souligné la nécessité pour les acteurs du secteur de la sécurité de développer des capacités de surveillance et de réaction à la cybercriminalité organisée. Ils ont également suggéré que le secteur de la sécurité peut jouer un rôle de premier plan dans la réponse aux cyberagressions « externes » ou « extraterritoriales » et contribuer à assurer la protection des infrastructures nationales critiques contre une cyberattaque majeure. Toutefois, les participants ont également souligné les nombreux risques qui découlent de l'implication du secteur de la sécurité dans la cybersécurité, tels que l'imposition de coûts inutiles si le secteur de la sécurité assume des responsabilités qu'il est préférable de laisser aux experts techniques du secteur privé ou d'autres branches du gouvernement, ou la réduction de la responsabilité du gouvernement si les acteurs du secteur de la sécurité ont accès à des informations privées ou les utilisent sans surveillance adéquate. Les participants ont suggéré que ces risques pourraient être atténués de la manière suivante :

   - *Favoriser les partenariats public-privé pour sécuriser les systèmes et infrastructures nationaux critiques contre les attaques.* En particulier lorsqu'il s'agit de sécuriser des secteurs fortement dépendants de la technologie tels que la banque, la finance et les télécommunications, les participants ont suggéré que le secteur privé est souvent le mieux placé pour jouer un rôle de premier plan dans la sécurité des réseaux, la surveillance des menaces et la récupération. Dans ces secteurs, les capacités du secteur privé dépassent généralement celles du gouvernement et des acteurs du secteur de la sécurité. Mais il y a aussi un rôle important pour les acteurs du gouvernement et du secteur de la sécurité qui, comme l'ont fait remarquer les participants, peuvent aider à identifier les infrastructures d'information critiques, faciliter l'échange d'informations entre les secteurs et mobiliser des ressources pour les secteurs manquant de moyens. En cas d'attaque majeure, les acteurs du secteur de la sécurité peuvent également mener des enquêtes, recueillir des preuves et inculper les responsables dans la juridiction de leur pays.

- *Renforcer ou créer des mécanismes de responsabilisation verticaux et horizontaux.* Les participants ont discuté de la façon dont les gouvernements ne peuvent pas compter sur des solutions techniques pour empêcher l'abus de données privées ou personnelles par des acteurs du secteur politique ou de la sécurité. Dans une large mesure, la garantie de la responsabilité nécessite l'existence, le renforcement ou la création de mécanismes de contrôle juridiques et institutionnels. Il s'agit notamment d'un pouvoir judiciaire et législatif indépendant, de médiateurs et d'inspecteurs généraux au sein de l'exécutif, ainsi que d'une société civile et de médias solides. Ces acteurs sont essentiels pour veiller à ce que les fonctionnaires soient tenus responsables, que les abus soient signalés et enregistrés, que les lois existantes soient respectées et que les lois ou politiques qui diminuent la transparence et la responsabilité du secteur de la sécurité soient modifiées ou annulées.

4. **La politique et la stratégie de cybersécurité en Afrique doivent être alignées sur les droits humains, l'État de droit et le respect de la sécurité des citoyens.** Aussi importante que soit la réponse à l'évolution rapide des cybermenaces sur le continent, les participants ont convenu de la nécessité de prendre en compte les conséquences de deuxième et troisième ordre des politiques visant à donner aux acteurs du secteur de la sécurité des outils pour lutter contre la criminalité organisée, le terrorisme ou l'espionnage liés à la cybernétique. Les participants ont souligné l'adoption généralisée de lois sur la cybercriminalité et la sécurité de l'information formulées en termes vagues, qui ont donné aux acteurs du secteur de la sécurité le pouvoir de censurer, surveiller et détenir des citoyens privés et des groupes d'opposition avec un contrôle limité. Le résultat net d'un grand nombre de ces lois a été de diminuer la confiance entre les citoyens et les États et de répandre des formes déstabilisantes et autoritaires de gouvernement. Au Mali, ces lois allaient à l'encontre de l'esprit de la constitution du pays et ont peut-être contribué au coup d'État d'août 2020 qui a éjecté du pouvoir le gouvernement élu du pays. Les participants ont suggéré que les décideurs politiques et les responsables du secteur de la sécurité en Afrique peuvent contribuer à faire en sorte que la cybersécurité soit alignée sur la sécurité des citoyens :

    - *Éviter l'ambiguïté.* Dans de nombreux cas, des termes tels que « désinformation » et « terrorisme » sont définis de manière vague ou d'une manière qui laisse aux gouvernements toute latitude pour criminaliser efficacement la liberté d'expression, en ciblant les manifestants non violents et l'opposition politique. L'utilisation large de ces termes dans la législation pénale doit être évitée.

    - *Renforcer le rôle de la société civile dans la politique et la stratégie de cybersécurité.* Les plénières et les groupes de discussion ont souligné le rôle que des organisations telles que le Kenya ICT Action Network (KICTANet) ont joué pour aider les gouvernements à comprendre les préoccupations de leur population et à mener des politiques de TIC centrées sur les citoyens. L'approche de KICTANet doit être reproduite à plus grande échelle. Pour les gouvernements, cela signifie des efforts plus actifs pour intégrer les groupes de la société civile dans la conception et la mise en œuvre de la politique des TIC. Pour les acteurs de la société civile, cela signifie se pencher sur un rôle de convocation et de coordination, plutôt que sur un rôle strictement axé sur le plaidoyer. Les participants ont encouragé les forces de sécurité à parler sur un pied d'égalité avec les citoyens, plutôt que de manière hiérarchique, ce qui peut faciliter leur travail en commun.

Regarder au-delà de l'horizon sur la sécurité du cyberespace en Afrique

Les échanges entre les participants et les panélistes au cours du programme ont également mis en lumière plusieurs éléments du paysage des cybermenaces en Afrique et des réponses des États qui méritent d'être analysés plus en profondeur par les chercheurs et de faire l'objet de discussions supplémentaires par les décideurs politiques locaux, régionaux et internationaux.

Les technologies de l'information comme technologie habilitante

Le domaine de la cybersécurité se concentre généralement sur la défense des réseaux contre les attaques qui compromettent la confidentialité, l'intégrité ou l'accès aux réseaux informatiques. L'accent mis sur la cybersécurité est un cadre important, mais également étroit, pour comprendre comment la diffusion des technologies de l'information a un impact sur la sécurité nationale en Afrique et ailleurs. En effet, la diffusion des technologies de l'information ne se contente pas de propager les vulnérabilités et les exploits informatiques, mais modifie également la manière dont les acteurs étatiques, les réseaux criminels organisés et les groupes extrémistes violents s'organisent, recrutent, se financent, communiquent et fournissent des biens et des services. La technologie de l'information est peut-être mieux conçue comme une technologie habilitante qui, comme l'électricité ou la vapeur, permet la croissance et la propagation d'autres technologies, comme les réseaux de paiement mobiles, l'intelligence artificielle, la fabrication additive et les véhicules aériens sans pilote. Dans la mesure où ces technologies deviennent de plus en plus sophistiquées, sont peu coûteuses et se diffusent rapidement, elles sont susceptibles d'avoir des conséquences profondes sur la paix, la stabilité et la sécurité en Afrique et au-delà.

Technologies de l'information et stratégie militaire

Les forces armées africaines ont parfois tenté de s'inspirer des armées plus dépendantes de la technologie dans les pays à revenu plus élevé. Les participants ont suggéré qu'il était temps de repenser cette approche et de mieux comprendre les risques, les vulnérabilités et les dépendances qui résultent de l'acquisition et de l'utilisation des technologies de l'information et des communications pour recueillir des renseignements, coordonner et permettre des opérations de combat. Le fait que l'infanterie africaine, par exemple, tende à être moins dépendante des technologies de l'information et de la communication que les forces armées d'autres régions du monde est, dans un sens, un avantage stratégique, qui la rend moins vulnérable aux cyberattaques. Les participants ont suggéré que les armées africaines doivent être en mesure d'utiliser la technologie de manière à pouvoir gagner dans les conflits centrés sur la population, ce qui pourrait signifier qu'il faut repenser les approches stratégiques, les doctrines opérationnelles, les structures des forces et les rôles des acteurs extérieurs. En outre, pour gagner dans une guerre hybride basée sur l'information, les forces de sécurité doivent établir des relations de coopération avec les citoyens et les acteurs privés afin de tirer parti de leurs capacités et de leur expertise.