AFRICA CENTER
FOR STRATEGIC STUDIES

PRIORIDADES DE SEGURANÇA DO CIBERESPAÇO PARA OS ATORES DE SEGURANÇA NACIONAL DE ÁFRICA
PROGRAMA ACADÉMICO VIRTUAL

SUMÁRIO EXECUTIVO

3 - 25 de agosto de 2021

De 3 a 25 de agosto de 2021, o Centro África de Estudos Estratégicos conduziu um programa online a nível executivo sobre o papel do setor da segurança na abordagem dos desafios e ameaças cibernéticas de África. Este sumário executivo fornece contexto, sintetiza as perspetivas dos participantes, partilha as principais perceções e identifica as tendências emergentes discutidas durante o programa. Os conhecimentos exploram a forma como o estado, o setor da segurança, o setor privado e os intervenientes da sociedade civil em África podem:

- Melhorar a sensibilização para as ameaças cibernéticas mais significativas e para os atores das ameaças
- Implementar abordagens multiparticipativas para a cibersegurança
- Aproveitar os benefícios e limitar os riscos de envolvimento do setor da segurança na cibersegurança
- Alinhar a política e estratégia de cibersegurança com os direitos humanos e o respeito pelo estado de direito

Contexto

O seminário reuniu participantes representando 30 países africanos com antecedentes civis e militares, bem como representantes selecionados do setor privado, sociedade civil e organizações regionais. Os objetivos eram que os participantes: i) expandissem a compreensão das ameaças e desafios relacionados com a cibersegurança em África, ii) identificassem prioridades-chave para os atores de segurança e defesa nacional na resposta à atividade cibernética maliciosa, e iii) discutissem como maximizar os benefícios da tecnologia da informação, minimizando ao mesmo tempo as ameaças e vulnerabilidades da cibersegurança.

A convocação de participantes de diferentes origens e de linhas militares e civis permitiu um diálogo holístico, respeitoso e informado sobre o papel do setor da segurança na cibersegurança em África. A primeira parte do programa centrou-se na compreensão do panorama da ameaça cibernética em África de uma perspetiva nacional orientada para a segurança. As restantes sessões discutiram os elementos-chave de uma resposta nacional de cibersegurança, centrando-se especificamente na resposta a incidentes de segurança informática, proteção de infraestruturas críticas e implementação de estratégias nacionais de cibersegurança.

Perspetivas dos Participantes sobre o Desafio

Os participantes discutiram como a rápida disseminação da tecnologia da informação está a tornar os seus países vulneráveis às ameaças da espionagem cibernética, sabotagem de infraestruturas críticas, crime organizado e inovação no combate. Discutiram como os agentes de ameaça mais significativos têm sido historicamente provenientes de agentes criminosos estatais e transnacionais externos a África, mas que existe uma preocupação crescente com a rápida disseminação de ameaças cibernéticas estratégicas do interior do continente. Numa sondagem conduzida durante a primeira sessão plenária, os participantes classificaram as redes criminosas organizadas e o extremismo violento como os atores da ameaça cibernética que mais os preocupam, em estreito paralelismo com as preocupações tradicionais de segurança que os responsáveis Africanos têm em relação a estes atores.

Além disso, os participantes salientaram a importância da necessidade de adotar uma lente de segurança centrada no cidadão ao gerir ameaças e desafios cibernéticos. Devido à natureza interna da maioria dos conflitos em África, o controlo e o acesso à população é muitas vezes tão importante como a violência física. Uma vez que a tecnologia da informação está a tornar-se cada vez mais central na forma como os estados informam, acedem e prestam serviços às suas populações, os governos devem utilizar a tecnologia da informação não só para enfrentar diretamente ameaças e vulnerabilidades, mas também para reforçar o contrato social entre governos e cidadãos.

Como podem os governos africanos equilibrar a necessidade do envolvimento do setor da segurança no ciberespaço, limitando simultaneamente os riscos e reforçando o contrato social? Os participantes ofereceram quatro ideias-chave.

Principais Perceções

1. **Os atores do governo, do setor da segurança, internacionais e do setor privado devem trabalhar em conjunto para melhorar a sensibilização para as ameaças cibernéticas mais significativas e para os atores da ameaça.** Praticamente todos os estados africanos possuem agora, no mínimo, uma unidade cibernética responsável pela monitorização e resposta ao cibercrime. No entanto, a consciência de como os agentes de ameaça mais desestabilizadores, tais como redes criminosas organizadas, grupos extremistas violentos e estados nacionais, estão a alavancar o ciberespaço e para que fins é mais limitada. Até os países africanos com maior maturidade cibernética permanecem numa fase bastante embrionária na determinação do papel que a tecnologia da informação deve desempenhar, se é que algum, na forma como o setor da segurança monitoriza e responde a estas ameaças, bem como o papel do setor da defesa como parte de uma resposta nacional mais ampla na área da cibersegurança. Os participantes sugeriram que a consciência das ameaças e desafios cibernéticos mais significativos do continente poderia ser melhorada através de:

    - *Sensibilização cibernética básica e desenvolvimento de capacidades em países com menos maturidade cibernética*. Os países com menos maturidade cibernética de África deveriam começar com formação básica de sensibilização cibernética e desenvolvimento de capacidades. O reforço das capacidades deve "ser a base da transformação digital e ser adaptada à importância da ameaça". Em países onde grandes faixas da população não têm acesso à Internet, estes esforços terão de ser conduzidos em conjunto com os esforços para melhorar a penetração da Internet e a literacia digital básica. Para os indivíduos com acesso à Internet, os participantes aconselharam a explorar formas de aumentar a consciencialização e de

reforçar capacidades a baixo custo, através de numerosos cursos e formações online gratuitas.

- *Monitorização e informação mais concertada sobre ameaças em países com maior maturidade cibernética*. Para os países que têm capacidade, os participantes sugeriram que eram necessários mais esforços para monitorizar, acompanhar e relatar as ameaças. Poucos países, por exemplo, publicam regularmente informações sobre o tipo e volume de ataques informáticos que experimentam, ou monitorizam as atividades online dos maiores e mais desestabilizadores agentes de ameaça. Muitas vezes, são terceiros que identificam e informam as partes afetadas de uma violação. Em parte, isto deve-se ao facto de a cibersegurança ser considerada uma questão sensível e tanto os governos como o setor privado estarem relutantes em denunciar ou revelar ataques. Ao sensibilizar todo o continente para o panorama da ameaça cibernética, os participantes sugeriram que é necessária muito mais transparência e colaboração para criar confiança entre múltiplos grupos de intervenientes, permitindo-lhes monitorizar, dissuadir e prevenir a atividade cibernética maliciosa.

2. **As respostas até mesmo às ameaças e desafios cibernéticos mais significativos precisam de ser informadas por uma abordagem multiparticipativa.** Ao contrário de outras tecnologias que são explicitamente concebidas para causar danos físicos, a tecnologia da informação tem uma vasta gama de utilizações, muitas ou a maioria das quais visam obter benefícios económicos e sociais. O capital humano, os conhecimentos técnicos e as capacidades de defesa no setor privado, especialmente nos setores financeiro e tecnológico, excedem geralmente os dos atores governamentais. Além disso, como a tecnologia da informação está a tornar-se cada vez mais essencial para a forma como os governos servem os seus cidadãos, tanto a indústria privada como as partes interessadas da sociedade civil têm um papel crucial a desempenhar na decisão da forma como a tecnologia da informação é utilizada. Foi notado que a cultura da defesa cibernética em toda a África tem de mudar, especialmente porque em muitos casos os civis são mais capazes do que os atores do setor da segurança na sua consciência cibernética e nível de formação. Os participantes destacaram como os ingredientes-chave para o sucesso da conceção e implementação da estratégia e política de cibersegurança multiparticipativa incluíram:

   - *Inclusividade e confiança.* A estratégia, legislação e conceção e implementação de políticas nacionais de cibersegurança devem procurar incluir e incorporar o feedback de "todos os intervenientes relevantes" na conceção, elaboração e implementação. Estes incluem, no mínimo: o setor da segurança, telecomunicações, finanças, energia, sociedade civil, academia e outros setores considerados essenciais para a proteção de infraestruturas críticas ciberdependentes. Os participantes notaram como a inclusividade ajuda a construir a confiança pública nas autoridades cibernéticas nacionais, permitindo a cooperação entre as várias partes interessadas e a comunicação de incidentes. Sem esta confiança pública, os esforços para combater as ameaças cibernéticas serão menos bem-sucedidos.

   - *Liderança política de alto nível.* Devido à variedade de intervenientes envolvidos, a estratégia e os processos políticos de cibersegurança não são geralmente eficazes sem uma liderança política de alto nível para atribuir papéis e responsabilidades e mediar disputas entre agências. No Gana, esta função foi assumida com um grupo de trabalho interministerial. Na Nigéria e no Burkina Faso, isto ficou à responsabilidade do National Security Advisor e da National Information System Security Agency (Agence Nationale de Sécurité des Systèmes

d'Information), respetivamente - duas entidades extraministeriais que reportam diretamente ao presidente.

- *Alavancagem da competência técnica.* A conceção e implementação de estratégias e políticas nacionais de cibersegurança precisam de ser informadas por peritos técnicos. No Níger, a Agência Nacional para as Redes de Informação (Agence Nationale pour la Société de l'Information) está a desempenhar um papel fundamental no desenvolvimento de uma estratégia nacional de cibersegurança e acabará por acolher a equipa de resposta a incidentes de segurança informática da nação (CSIRT). No Gana, este papel é desempenhado por um grupo de trabalho técnico encarregue de implementar políticas cibernéticas nacionais e de fazer recomendações ao comité interministerial. O CSIRT nacional do Gana tem também desempenhado um papel importante no estabelecimento e coordenação dos esforços dos CSIRT regionais e setoriais, que continuam a ser raros em África.

3. **O setor da segurança tem um papel crucial a desempenhar na segurança do ciberespaço, mas que comporta riscos, bem como benefícios.** Embora concordando que não existe uma abordagem de formato único, houve um consenso de que o setor da segurança em África tinha um papel crucial a desempenhar como parte de uma resposta nacional mais ampla em matéria de cibersegurança. Os participantes salientaram a necessidade de os atores do setor da segurança desenvolverem a capacidade de controlar e responder ao crime organizado cibernético. Sugeriram também que o setor da segurança pode desempenhar um papel de liderança na resposta à agressão cibernética "externa" ou "extraterritorial" e ajudar a assegurar a proteção de infraestruturas nacionais críticas contra um grande ataque cibernético. No entanto, os participantes também destacaram numerosos riscos que decorrem do envolvimento do setor da segurança na cibersegurança, tais como a imposição de custos desnecessários se o setor da segurança assumir melhor as responsabilidades deixadas a especialistas técnicos do setor privado ou outros ramos do governo; ou reduções na responsabilização do governo se os atores do setor da segurança tiverem acesso ou utilizarem informação privada sem supervisão adequada. Os participantes sugeriram que estes riscos poderiam ser mitigados através das seguintes formas:

    - *Fomento de parcerias público-privadas para assegurar sistemas e infraestruturas nacionais críticas contra ataques.* Particularmente quando se trata de garantir setores fortemente dependentes da tecnologia, tais como a banca, finanças e telecomunicações, os participantes sugeriram que o setor privado é muitas vezes o mais adequado para assumir um papel de liderança na segurança de redes, monitorização de ameaças e recuperação. Nestas áreas, as capacidades do setor privado ultrapassam geralmente as dos atores do governo e do setor da segurança. Mas há também um papel importante para os atores governamentais e do setor da segurança, que, como os participantes observaram, podem ajudar a identificar infraestruturas de informação críticas, facilitar a troca de informação entre setores e mobilizar recursos para setores com poucos recursos. No caso de um grande ataque, os agentes do setor da segurança podem também conduzir investigações, recolher provas e acusar os responsáveis na jurisdição do seu país.

    - *Reforço ou criação de mecanismos de responsabilização verticais e horizontais.* Os participantes discutiram como os governos não podem confiar em soluções técnicas para evitar o abuso de dados privados ou pessoais por parte de atores políticos ou do setor da segurança. Em

grande medida, assegurar a responsabilização requer a existência, reforço ou criação de mecanismos de supervisão jurídica e institucional. Estas medidas incluem um poder judicial e legislativo independente; provedores e inspetores-gerais dentro do ramo executivo; e uma sociedade civil e meios de comunicação social robustos. Tais atores são essenciais para assegurar que os funcionários sejam responsabilizados, que os abusos sejam denunciados e registados, que as leis existentes sejam seguidas e que as leis ou políticas que diminuem a transparência e a responsabilização do setor da segurança sejam modificadas ou derrubadas.

4. **A política e estratégia de cibersegurança em África precisa de ser alinhada com os direitos humanos, o estado de direito e o respeito pela segurança dos cidadãos.** Por muito importante que seja responder à rápida evolução do leque de ameaças cibernéticas do continente, os participantes concordaram na necessidade de considerar as consequências de segunda e terceira ordem das políticas destinadas a dar aos atores do setor da segurança instrumentos para combater o crime organizado relacionado com o ciberespaço, o terrorismo ou a espionagem. Os participantes apontaram para a adoção generalizada de leis de cibercriminalidade e de segurança da informação com redação vaga, que deram aos atores do setor da segurança autoridade para censurar, controlar e deter cidadãos privados e grupos da oposição com supervisão limitada. O resultado líquido de muitas destas leis tem sido a diminuição da confiança entre cidadãos e estados e a difusão de formas de governo desestabilizadoras e autoritárias. No Mali, tais leis foram contra o espírito da constituição do país e podem ter contribuído para o golpe de estado de agosto de 2020, que expulsou do poder o governo eleito do país. Os participantes sugeriram que os decisores políticos e responsáveis do setor de segurança em África possam ajudar a garantir que a segurança cibernética esteja alinhada com a segurança dos cidadãos:

    - *Evitando ambiguidades.* Em muitos casos, termos como "desinformação" e "terrorismo" são vagamente definidos ou definidos de forma a dar aos governos a liberdade necessária para criminalizar efetivamente a liberdade de expressão, visando os manifestantes não violentos e a oposição política. A ampla utilização de tais termos na legislação penal deve ser evitada.

    - *Elevação do papel da sociedade civil na política e estratégia de cibersegurança.* Grupos plenários e de discussão destacaram o papel que organizações como a Kenya ICT Action Network (KICTANet) têm desempenhado para ajudar os governos a compreender as preocupações do seu povo e a prosseguir políticas de TIC centradas no cidadão. A abordagem do KICTANet precisa de ser mais amplamente replicada. Para os governos, isto significa esforços mais ativos para incorporar grupos da sociedade civil na conceção e implementação da política das TIC. Para os atores da sociedade civil, significa inclinar-se para um papel de convocação e coordenação, que se centra estritamente na advocacia. Os participantes encorajaram as forças de segurança a falar em pé de igualdade com os cidadãos, em vez de hierarquicamente, podendo facilitar o seu trabalho em conjunto.

O horizonte da Segurança do Ciberespaço em África

Os intercâmbios de participantes e de membros de painéis durante o programa também destacaram vários elementos do panorama da ameaça cibernética em África e respostas estatais que merecem uma análise mais aprofundada por parte dos investigadores e discussões adicionais por parte dos decisores políticos locais, regionais e internacionais.

A tecnologia da informação como tecnologia capacitadora

O campo da cibersegurança centra-se tipicamente na defesa de redes contra ataques que comprometem a confidencialidade, integridade ou o acesso a redes informáticas. O foco na cibersegurança é um quadro importante, mas também estreito, para compreender como a disseminação da tecnologia da informação está a ter impacto na segurança nacional em África e noutros locais. Isto porque a disseminação da tecnologia da informação não só espalha vulnerabilidades e explorações informáticas, mas também está a mudar a forma como os atores estatais, redes criminosas organizadas e grupos extremistas violentos se organizam, recrutam, financiam, comunicam e entregam bens e serviços. A tecnologia da informação é talvez mais bem concebida como uma tecnologia que, tal como a eletricidade ou a energia a vapor, permite o crescimento e a difusão de outras tecnologias, tais como redes de pagamento móveis, inteligência artificial, fabrico de aditivos e veículos aéreos não tripulados. Na medida em que estas tecnologias crescem em sofisticação, são de baixo custo e se difundem rapidamente, é provável que tenham consequências profundas para a paz, estabilidade e segurança em África e não só.

Tecnologia da informação e estratégia militar

As forças armadas africanas, por vezes, tentaram modelar-se a partir de exércitos mais dependentes da tecnologia em países de rendimento mais elevado. Os participantes sugeriram que era altura de repensar esta abordagem e de compreender melhor os riscos, vulnerabilidades e dependências resultantes da aquisição e utilização das tecnologias de informação e comunicação para recolher informações, coordenar e permitir operações de combate. O facto de a infantaria africana, por exemplo, tender a ser menos dependente das tecnologias de informação e comunicação do que as forças armadas noutras partes do mundo é, em certo sentido, uma vantagem estratégica, tornando-as menos vulneráveis a ataques cibernéticos. Os participantes sugeriram que os exércitos africanos precisam de ser capazes de empregar tecnologia que lhes permita vencer em conflitos centrados na população, o que poderia significar repensar abordagens estratégicas, doutrinas operacionais, estruturas de força e papéis para atores externos. Além disso, para vencer na guerra híbrida, baseada na informação, as forças de segurança precisam de estabelecer relações de cooperação com cidadãos e atores privados para alavancar as suas capacidades e perícia.