CENTRO ÁFRICA
DE ESTUDOS ESTRATÉGICOS

Prioridades de Segurança do Ciberespaço para os Agentes da Segurança Nacional de África

PROGRAMA DE CURSO

Online, via Zoom para o Governo

3 – 25 de Agosto de 2021

CENTRO ÁFRICA
DE ESTUDOS ESTRATÉGICOS

PRIORIDADES DE SEGURANÇA DO CIBERESPAÇO PARA OS AGENTES DA SEGURANÇA NACIONAL DE ÁFRICA

3 – 25 de Agosto de 2021

Online, via Zoom para o Governo

PROGRAMA DE CURSO

ÍNDICE

SOBRE O CENTRO África

Desde a sua criação, em 1999, o Centro África tem servido como um fórum para pesquisa, programas académicos e troca de ideias, com o objectivo de melhorar a segurança dos cidadãos através do reforço da eficácia e da responsabilização das instituições africanas, em apoio à política E.U.A - África.

VISÃO

Segurança para todos os africanos defendida por instituições eficazes e responsabilizáveis perante os seus cidadãos.

A principal motivação do Centro África é a concretização da visão de uma África livre da violência armada organizada, garantida por instituições africanas empenhadas em proteger os cidadãos africanos. Este objetivo sublinha o compromisso do Centro em contribuir para impactos tangíveis, trabalhando com os nossos parceiros africanos militares e civis, governamentais e da sociedade civil, bem como nacionais e regionais. Todos têm papéis importantes a desempenhar na atenuação dos complexos fatores de conflito que existem atualmente no continente. A responsabilização perante os cidadãos é um elemento importante da nossa visão, pois reforça o ponto de vista de que, para serem eficazes, as instituições de segurança devem ser não só "fortes", mas também sensíveis aos direitos dos cidadãos e protetoras dos mesmos.

MISSÃO

Fazer avançar a segurança africana através da expansão do conhecimento, do fornecimento de uma plataforma de confiança para o diálogo, da criação de parcerias duradouras e do desencadeamento de soluções estratégicas.

A missão do Centro África centra-se na produção e disseminação do conhecimento através da nossa investigação, programas académicos, comunicações estratégicas e delegações comunitárias. Com base nas experiências práticas e lições aprendidas através dos esforços de segurança no continente, pretendemos gerar uma visão e análise relevantes, que possam informar os profissionais e os decisores políticos sobre os prementes desafios de segurança que enfrentam. Reconhecendo que enfrentar desafios sérios só pode acontecer através de trocas francas e ponderadas, o Centro fornece plataformas presenciais e virtuais onde os parceiros podem trocar opiniões sobre prioridades e boas práticas. Estas trocas promovem relacionamentos que, por sua vez, são mantidos ao longo do tempo através das delegações comunitárias do Centro, comunidades de interesse, programas de acompanhamento e diálogo contínuo entre participantes e funcionários. Este diálogo, alimentado com experiências do mundo real e novas análises, proporciona uma oportunidade para a aprendizagem contínua e catalisa ações concretas.

MANDATO

O Centro África é uma instituição do Departamento de Defesa dos Estados Unidos criada e financiada pelo Congresso para o estudo de questões de segurança relacionadas com a África e serve como um fórum para investigação, comunicação, troca de ideias e formação bilaterais e multilaterais, envolvendo participantes militares e civis. *(10 U.S.C 342)*

MAPA DE ÁFRICA

Map No. 4045 Rev. 7 UNITED NATIONS
November 2011

Department of Field Support
Cartographic Section

VISÃO GERAL

O aumento da penetração da internet e a rápida inovação na tecnologia digital estão a ampliar a natureza dos desafios de segurança em África. Os governos africanos, os agentes do sector da segurança e os seus cidadãos são vulneráveis a uma série de vastas ameaças cibernéticas em evolução, provenientes de uma variedade de intervenientes estatais, não estatais e criminosos. A proliferação de sensores de baixo custo, tecnologia de vigilância e *malware* sofisticado levou o ciberespaço a tornar-se no meio predominante de espionagem patrocinada pelo Estado. A crescente dependência tecnológica torna infraestruturas críticas, tais como sistemas militares, redes governamentais e sectores como a energia e a banca vulneráveis à sabotagem cibernética. Surgem alterações na estruturação e financiamento das formas mais tradicionais de crime organizado, paralelamente ao aparecimento de novas formas de crime organizado digital. A disseminação das tecnologias de informação também tem implicações na forma como os intervenientes estatais e não estatais violentos recrutam, se organizam e se financiam, bem como, nas estratégias e táticas que utilizam para exercer violência.

Apesar destas crescentes ameaças e vulnerabilidades, o sector de segurança africano tem estado largamente ausente dos esforços nacionais e regionais destinados a melhorar a segurança do ciberespaço. No entanto, o sector da segurança tem um papel crucial a desempenhar na segurança dos sistemas e redes governamentais, impedindo a propagação do cibercrime organizado, protegendo infraestruturas nacionais críticas de ataques cibernéticos e respondendo a outras utilizações maliciosas das tecnologias de informação por intervenientes organizados e violentos. Crucialmente, uma política eficaz de segurança do ciberespaço requer cooperação e coordenação entre as várias partes interessadas. Grande parte da inovação, perícia e capital humano necessários para a maturidade da segurança do ciberespaço cabe ao sector privado. A supervisão por parte dos intervenientes civis e da sociedade civil é necessária para assegurar que as políticas de segurança cibernética se encontrem alinhadas com princípios sólidos de governação do sector da segurança Para se manterem à frente das ameaças de amanhã, os governos de todo o continente terão de adoptar uma abordagem colaborativa, de todo o governo e centrada no cidadão, para a segurança do ciberespaço.

OBJETIVOS DO PROGRAMA:

1. Expandir a compreensão dos principais desafios que as tecnologias de informação interdependentes colocam à segurança nacional e cidadãos nos países africanos.

2. Identificar as principais prioridades dos intervenientes africanos da defesa e segurança para melhor se prepararem e responderem às atividades cibernéticas perniciosas, que ameaçam os interesses da segurança nacional.

3. Comparar experiências, perspectivas e boas práticas na política de segurança do ciberespaço numa série de sectores de segurança, sociedade civil, sector privado e partes interessadas não governamentais.

4. Socializar os benefícios de manter uma internet aberta, fiável e segura para otimizar as vantagens das tecnologias de informação interdependentes para as empresas, governos

e sociedades, reduzindo ao mesmo tempo as ameaças e vulnerabilidades de segurança do ciberespaço.

FORMATO DO PROGRAMA:

Cada semana, o programa irá incluir (1) uma sessão plenária composta por um debate moderado com um conjunto de especialistas - desde decisores políticos a profissionais especializados e académicos - seguido de uma sessão interativa de perguntas e respostas; e (2) debates em pequenos grupos para os participantes discutirem as suas reações à sessão plenária e partilharem experiências uns com os outros.

O programa será realizado em inglês, francês e português. A fim de fomentar discussões francas e criar confiança entre os participantes, os debates serão conduzidos de acordo com uma política de não atribuição, o que significa que os comentários e as intervenções específicas dos participantes não serão, de modo algum, identificados pelo nome nem pelo país em quaisquer resumos, relatórios ou partilha dos conhecimentos adquiridos no decorrer do seminário por parte de qualquer participante, orador ou organizador.

PROGRAMA DE CURSO:

O presente programa de curso fornece uma visão geral dos objetivos académicos e das principais questões políticas que este programa procura levantar relativamente às prioridades do sector de segurança africano na segurança do ciberespaço em África. Para cada sessão, o programa oferece uma breve introdução e apresenta as questões para discussão. Também incluímos artigos selecionados, cujo objetivo principal é ajudar a enquadrar as questões no contexto das bolsas de estudo e dos documentos de política disponíveis. É provável que o programa abranja mais questões e materiais do que aqueles que podem ser suficientemente debatidos no tempo disponível. Será proveitoso ler alguns ou todos os materiais de leitura recomendados no programa de curso antes do seminário, porque as leituras vão enquadrar os comentários dos participantes e dos oradores no contexto apropriado. Contudo, esperamos também que utilize estes materiais como recursos mesmo após a conclusão do programa, e que volte a eles para obter pormenores relevantes.

Os materiais externos e o conteúdo académico do presente programa de curso não refletem a posição oficial do Departamento de Defesa nem do governo dos EUA. O presente curso consiste num documento educativo que pretende expor os participantes a várias perspectivas, no sentido de os ajudar a tirar o máximo proveito do programa.

PREPARAÇÃO DO PROGRAMA:

Antes do seminário, recomendamos o seguinte:

1. Ler o presente programa de curso.

2. Ler a bibliografia e ver os vídeos recomendados.

3. Dedicar algum tempo à reflexão e resposta às questões do debate.

4. Considerar quais as experiências do seu trabalho que podem ser relevantes para a partilha em grupos de debate.

5. Estar preparado para participar ativamente em grupos de discussão e aprender com participantes de outros países.

Sessão plenária 1: Panorama das ameaças cibernéticas em África

OBJETIVOS:

- Descrever o âmbito e a escala das ciberameaças que os países africanos enfrentam em resultado de espionagem, sabotagem de infraestruturas críticas, crime organizado e luta contra a inovação.

- Explorar como a natureza das ameaças cibernéticas africanas provavelmente mudará e evoluirá no futuro.

- Considere o escopo e a escala dessas ameaças cibernéticas na África do Sul

ENQUADRAMENTO:

A rápida difusão das tecnologias de informação e comunicação (TIC) está a reformular o panorama da segurança em África. Embora a digitalização tenha trazido enormes benefícios económicos e sociais, também está a ampliar e a alterar a natureza dos desafios de segurança do continente. Todas as redes informáticas, redes locais (LANs), e redes de área ampla (WANs) são vulneráveis a tentativas de violação da confidencialidade, alteração da integridade ou perturbação do acesso à informação armazenada no seu interior. Mais amplamente, a difusão das TIC está a alterar a forma como e por quem a informação é processada, armazenada, e divulgada. Estes aspectos da tecnologia digital permitem que ela seja explorada para fins nefastos por redes criminosas, grupos terroristas, hackers solitários e estados-nação rivais, entre outros intervenientes maliciosos. Quanto maior for o grau de conectividade, mais os países africanos e os seus cidadãos correm o risco de ter as suas tecnologias viradas contra eles.

As ameaças e os desafios cibernéticos centrais de África incluem:

- **Espionagem e vigilância.** Os sistemas de informação transformaram decisivamente os métodos e as fontes que os estados-nação, empresas e intervenientes não estatais utilizam para recolher e proteger informação sensível. Embora as preocupações mais significativas relativamente à espionagem cibernética em África se tenham centrado em torno de intervenientes estrangeiros, as capacidades de espionagem e vigilância estão a difundir-se rapidamente por todo o continente.

- **Sabotagem de infraestruturas críticas.** As redes governamentais, sistemas militares, bancos e setores de telecomunicações de África são vulneráveis a ciberataques que procuram incapacitá-los ou destruí-los. Os países africanos são particularmente vulneráveis, dado que a maioria das infraestruturas de TIC do continente é fornecida por intervenientes externos e os sectores-chave tais como eletricidade, água e energia possuem, frequentemente, pontos únicos de falha.

- **Crime organizado**: A expansão do ciberespaço levou à formação de formas inteiramente novas de redes de crime organizado, que exploram as ferramentas digitais para roubar, transferir e extorquir recursos. Nos últimos anos, o continente africano cresceu, como alvo e

como fonte de crime organizado cibernético. De forma igualmente crucial, a difusão das TIC está também a influenciar a forma como as empresas tradicionais do crime organizado, tais como o tráfico humano, o terrorismo, o extremismo violento, a criminalidade no mar e o tráfico de armas se estruturam e financiam.

- **Combate à inovação.** A tecnologia da informação está a tornar-se cada vez mais central na forma como a segurança é gerida e entregue aos cidadãos, incluindo estratégias, operações e táticas de segurança. Como as instituições e os intervenientes da segurança em todo o continente procuram beneficiar das capacidades de vigilância reforçadas e das tecnologias emergentes, tais como os *drones*, os intervenientes não estatais estão a explorar tecnologias emergentes para angariar fundos, recrutar, organizar e cometer atos de violência.

QUESTÕES PARA DEBATE:

- O que considera serem as principais ameaças e desafios cibernéticos no seu país ou região? Qual a sua gravidade?

- Que sectores no seu país ou região são mais vulneráveis aos ciberataques?

- Como vê o panorama das ameaças cibernéticas no seu país ou região a evoluir nos próximos cinco ou dez anos?

LEITURA RECOMENDADA:

Nathaniel Allen, "Africa's Evolving Cyber Threats," Centro África de Estudos Estratégicos, 19 de janeiro de 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," Comité Internacional da Cruz Vermelha, 17 de junho de 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, dezembro de 2019.
https://www.policycenter.ma/sites/default/files/PP_19-20_Al-Manir.pdf

ENACT and INTERPOL, *Online Organized African Crime from the Surface to the Darkweb*, INTERPOL Analytical Report, julho de 2020.
https://enact-africa.s3.amazonaws.com/site/ uploads/2020-08-20-interpol-darkweb-report%20.PDF

African Union and Symantec, *Cyber Crime and Cyber Security Trends in Africa*, nevembro de 2016.
https://thegfce.org/wp-content/uploads/2020/06/CybersecuritytrendsreportAfrica-en-2.pdf

VÍDEOS RECOMENDADOS:

Centro África de Estudos Estratégicos, “Emerging Cyber Dimensions of Africa’s Security Landscape,” (Dimensões Cibernéticas Emergentes da Paisagem de Segurança de África) 3 de dezembro de 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/

Centro África de Estudos Estratégicos, “Dimensões Cibernéticas do Aparelho de Estado em África,” 18 de março de 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/

Centro África de Estudos Estratégicos, "Cyber Dimensions of Violent Extremism in Africa," 19 de maio de 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/

Centro África de Estudos Estratégicos, "Dimensões Cibernéticas do Crime Organizado Transnacional em África," 8 de julho de 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/

Sessão Plenária 2: Elementos fundamentais de uma resposta nacional de segurança do ciberespaço

OBJETIVOS:

- Identificar os elementos principais da resposta a nível nacional necessários para enfrentar os desafios à segurança nacional relacionados com o ciberespaço.

- Identificar os principais intervenientes e as partes interessadas na concepção e concretização de uma resposta nacional à segurança do ciberespaço e o papel dos intervenientes da segurança nacional no âmbito de uma abordagem multilateral.

- Avaliar a política, estratégia e instituições de segurança do ciberespaço dos principais países africanos, a nível nacional.

- Fazer um balanço do papel do sector da segurança nos esforços nacionais para enfrentar as ameaças cibernéticas de espionagem, sabotagem de infraestruturas críticas, crime e combate à inovação.

- Discutir os benefícios de manter uma internet aberta, fiável e segura para otimizar as vantagens das tecnologias de informação interdependentes para as empresas, governos e sociedades, reduzindo ao mesmo tempo as ameaças e vulnerabilidades de segurança do ciberespaço.

ENQUADRAMENTO:

As estratégias e políticas de cibersegurança encontram-se numa fase incipiente em grande parte de África. A maioria dos países africanos não possui estratégias de cibersegurança nem equipas nacionais de resposta a incidentes informáticos, o mínimo necessário para uma infraestrutura nacional básica de gestão de ameaças cibernéticas. Nos principais países, o papel do sector da segurança enquanto parte de uma resposta mais ampla de cibersegurança varia substancialmente. No Quénia, no Senegal e nas Maurícias, os ministérios das telecomunicações são os principais organismos responsáveis pela supervisão da política de cibersegurança. Na Nigéria e na África do Sul, o sector da segurança assumiu um papel mais importante: os organismos que lideram o setor são o Conselheiro Nacional de Segurança e a Agência de Segurança do Estado, respectivamente.[1]

Abordar a evolução das ameaças cibernéticas do continente requer uma resposta abrangente, liderada pelos governos. Os elementos principais desta resposta incluem:[2]

a) Estratégias nacionais, que articulam a visão de cibersegurança e os objetivos estratégicos, e definem e estabelecem prioridades em relação aos desafios mais críticos de cibersegurança de um país, canalizam recursos, atribuem responsabilidades de

[1] Um repositório das estratégias nacionais de cibersegurança de cada país pode ser encontrado no sítio da internet da União das Telecomunicações em https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.

[2] Para um enquadramento internacionalmente aceite, ver, por exemplo, the Oxford Cyber Maturity Model: https://gcscc.ox.ac.uk/cmm-dimensions-and-factors#collapse2008981

cibersegurança a nível governamental e asseguram a supervisão civil dos agentes de segurança.

b) Quadros jurídicos e regulatórios para abordar o crescente cibercrime organizado e aumentar a capacidade dos organismos de aplicação da lei para utilizar provas digitais.

c) Equipas de resposta a incidentes informáticos e de gestão de crises, que podem identificar, monitorizar e proteger as infraestruturas de informação nacionais críticas e ajudar na recuperação de inevitáveis violações de segurança.

d) Consciência cibernética do sector de segurança nacional, identificação de ameaças e capacidade de resposta.

Independentemente do país ou contexto, a coordenação entre as várias partes interessadas é fundamental para uma resposta nacional eficaz. O sector privado, a sociedade civil e os agentes de segurança são parceiros fundamentais e não opositores nem obstáculos para o governo ou para os organismos do setor da segurança que atuam para desenvolver abordagens nacionais sólidas à segurança do ciberespaço. Os governos de toda a África dependem do sector privado para fornecer a mais recente tecnologia em cibersegurança, para relatar incidentes, monitorizar ameaças, e para assumir um papel de liderança na segurança dos sectores-chave contra os ciberataques, tais como as telecomunicações e a banca. A sociedade civil é um interveniente igualmente essencial para garantir que a política de cibersegurança se mantenha coerente com os direitos humanos, a democracia e a segurança dos cidadãos. O sucesso das organizações como a Kenya ICT Action Network[3] na promoção do diálogo público e no impulsionamento de reformas no sector das TIC ilustra a importância de uma abordagem multilateral à segurança do ciberespaço.

O mais importante é a forma como a política e a estratégia de segurança cibernética são formuladas e executadas. Com pouco envolvimento por parte do sector da segurança, um país pode não conseguir contar com redes governamentais sensíveis, desenvolver a capacidade necessária para monitorizar e responder ao crime organizado e integrar a tecnologia digital nas suas estratégias, operações e táticas militares. Uma presença excessiva por parte do sector de segurança, contudo, pode criar custos desnecessário e reduzir a supervisão civil, bem como a responsabilização. Qualquer que seja o seu papel é essencial que o governo e os intervenientes do sector da segurança tenham em mente que a segurança dos cidadãos é fundamental para a cibersegurança. Devem orientar os esforços no sentido de responder às ameaças colocadas pela disseminação da tecnologia digital de harmonia com os valores consagrados na Arquitetura de Paz e Segurança Africana: Estado de direito, direitos humanos e democracia.

QUESTÕES PARA DEBATE:

- Qual é a eficácia do seu país/região na resposta às ameaças cibernéticas e quais são os desafios?

- Que papel desempenha o sector da segurança na segurança do ciberespaço do seu país? Que outros intervenientes participam na segurança do ciberespaço no seu país?

[3] Para mais informações sobre a Kenya ICT Action Network, consultar: https://www.kictanet.or.ke/about-kictanet/

- Que papel deverá ter o sector da segurança no que diz respeito a enfrentar as ameaças e os desafios cibernéticos do seu país? De que forma isso poderia apoiar uma abordagem multilateral?

- Quais são os desafios e os riscos associados ao envolvimento do sector de segurança na segurança do ciberespaço?

LEITURA RECOMENDADA:

Global Cyber Security Capacity Centre, "Cyber Maturity Model Dimension 1: Cybersecurity Policy and Strategy,"Oxford University.
https://gcscc.ox.ac.uk/cmm-dimensions-and-factors#collapse2008981

Global Forum on Cyber Expertise, "Dehli Communiqué on a GFCE Agenda for Global Cyber Capacity Building," 24 de novembro de 2017.
https://thegfce.org/wp-content/uploads/2020/04/ DelhiCommunique.pdf

United Nations Information Technology Union, "2020 Global Cybersecurity Index," United Nations, 29 de junho de 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" em *Guide to Good Governance in Cybersecurity,"* p. 25-38, janeiro de 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.pdf

"A Problemática Da Cibersegurança E Os Seus Desafios," Centro de I&D Sobre direito e sociedade, setembro de 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," Brookings Techstream Blog, 11 de março de 2021.
https://www.brookings.edu/techstream/the-promises-and-perils-of-africas-digital-revolution/

Sessão plenária 3: Gestão de incidentes cibernéticos e proteção de infraestruturas críticas

OBJETIVOS:

- Definir infraestruturas críticas e examinar a escala e o âmbito das ameaças e vulnerabilidades do ciberespaço nos países africanos

- Debater o papel das Equipas de Resposta a Incidentes de Segurança Informática (CSIRT) nacionais e sectoriais como parte de um sistema nacional de resposta de cibersegurança para identificar e responder a ataques cibernéticos maliciosos a infraestruturas críticas.

- Debater o papel que os intervenientes da segurança nacional desempenham enquanto elementos principais das CSIRT, das células de coordenação interagências e de outros mecanismos de cooperação interagências para a segurança do ciberespaço.

- Explorar a melhor forma de promover as parcerias intersectoriais entre civis, agentes de segurança, forças policiais, justiça e parceiros do sector privado para salvaguardar as infraestruturas críticas dependentes da Internet.

ENQUADRAMENTO:

À medida que os países africanos se desenvolvem e digitalizam, os seus sistemas de infraestruturas críticas (IC), serviços e bens tornar-se-ão cada vez mais vulneráveis aos ciberataques. A União Internacional das Telecomunicações (UIT) fornece uma definição orientadora das infraestruturas críticas como "os principais sistemas, serviços e funções cuja perturbação ou destruição teria um impacto debilitante na saúde pública e na segurança, no comércio e na segurança nacional ou em qualquer combinação destes".[4] Como parte das infraestruturas críticas, a Infraestrutura de Informação Crítica (IIC) inclui as infraestruturas críticas de telecomunicações, bem como os sistemas TIC necessários para o funcionamento completo das infraestruturas críticas em múltiplos sectores.[5] As infraestruturas críticas de informação funcionam entre uma rede de sectores interligados e interdependentes, onde os sistemas TIC contêm vulnerabilidades inerentes que podem ser exploradas por meio de ataques aos sistemas de informação de controlo de uma infraestrutura. Os ataques a estes "sistemas de controlo", nomeadamente os sistemas de controlo e aquisição de dados de supervisão (SCADA) e de comando de incidentes (ICS) podem produzir um efeito de propagação de danos a outras infraestruturas críticas.

A cibersegurança das infraestruturas críticas envolve esforços sustentados para proteger os ativos das infraestruturas críticas de ataques externos, juntamente com esforços sustentados para apoiar a continuidade dos serviços de infraestruturas, quando ocorrem incidentes de segurança informática. As Equipas de Resposta a Incidentes de Segurança Informática (CSIRT) são um

[4] Grupo de Estudo da UIT Q.22/1 Relatório sobre as Melhores Práticas para uma Abordagem Nacional da Cibersegurança: A Management Framework for Organizing National Cybersecurity Efforts, ITU-D Secretariat, Geneva (2008).
[5] Maglaras, Leandros, et al. "Threats, countermeasures and attribution of cyber attacks on critical infrastructures." (Ameaças, contramedidas e atribuição de ciberataques a infraestruturas críticas). EAI Endorsed Transactions on Security and Safety 5.16 (2018).

mecanismo integral de proteção de infraestruturas críticas de informação, permitindo a gestão de incidentes e respostas a emergências, bem como a monitorização do ambiente de ameaça, e a resposta e a recuperação de grandes ciberataques. A nível nacional, as equipas CSIRT prestam serviços amplos e extensivos ao país, trabalhando em estreita colaboração com equipas CSIRT sectoriais e do sector privado, permitindo o intercâmbio de informação e uma comunicação oportuna e relevante.

Os países africanos enfrentam tanto oportunidades como limitações quando se trata de proteger infraestruturas críticas contra ataques cibernéticos. Por um lado, um nível limitado de dependência tecnológica, em comparação com as regiões mais industrializadas do mundo, bem como a escassez de sistemas antigos, proporciona a muitas nações africanas a oportunidade de integrar a cibersegurança nas suas redes de infraestruturas a partir do zero. Por outro lado, a elevada dependência em intervenientes externos para o fornecimento de infraestruturas críticas, a existência de pontos únicos de falha e investimentos limitados em segurança cibernética das infraestruturas críticas representam riscos significativos. Apenas 22 países africanos possuem equipas de CSIRT nacionais,[6] em parte devido ao tempo intensivo, aos investimentos financeiros e aos recursos técnicos de que necessitam. [7] A existência de CSIRT a nível sectorial é rara, em parte devido à presença de pequenas e médias empresas e organizações, que enfrentam limitações de recursos semelhantes.

QUESTÕES PARA DEBATE:

- O que caracterizaria como infra-estrutura crítica no seu país ou região? Até que ponto é que esta infra-estrutura crítica é ciberdependente?
- O seu país tem equipas de CSIRT, e até que ponto elas são eficazes na proteção de infraestruturas cibercríticas?
- Que leis, políticas ou mecanismos é que o seu país tem em vigor para proteger as infraestruturas nacionais críticas contra ataques cibernéticos?
- Que papel é que o sector da segurança tem na proteção das infra-estruturas nacionais críticas do seu país?
- Como é que a cooperação, a coordenação e a partilha de informação entre o sector da segurança, outras partes do governo e as partes interessadas fora do governo pode ser melhorada, de modo a aumentar a resiliência das infraestruturas nacionais ciberdependentes?

LEITURA RECOMENDADA:

Nathaniel Allen and Noelle van der Waag-Cowling, "How African Countries Should Address State-Sponsored Cyber Threats," Brookings Techstream Blog, 15 de julho, 2021

[6] Consulte os últimos dados da União das Tecnologias de Informação: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

[7] Mouton, Jean, and Ian Ellefsen. "The identification of information sources to aid with critical information infrastructure protection." 2013 Information Security for South Africa (2013): 1-8.

https://www.brookings.edu/techstream/how-african-states-can-tackle-state-backed-cyber-threats/

Internet Society and the African Union Commission, "Internet Infrastructure Guidelines for Africa," 24 de março de 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, "Segurança cibernética deve ser prioridade para setor de infraestrutura crítica," 20 de setembro de 2020
https://revistadigitalsecurity.com.br/seguranca-cibernetica-deve-ser-prioridade-para-setor-de-infraestrutura-critica/

Hanneke Duijnhoven, Bram Poppink, Tom van Schie, and Don Stikvoort, "Getting Started with a National Computer Security Incident Response Team (CSIRT) Guide," Netherlands Organisation for Applied Scientific Research, 2021.
https://cybilportal.org/tools/getting-started-with-a-national-csirt-guide/

Eric Luiijf, Tom van Schie, Theo van Ruijven, and Auke Huistra, "The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers," GFCE-Meridian, 2016.
https://www.tno.nl/media/8578/gpg_criticalinformationinfrastructureprotection.pdf

Sessão plenária 4: Estratégia nacional de cibersegurança

OBJETIVOS:

- Debater o processo de elaboração de uma estratégia nacional de segurança do ciberespaço e identificar os seus elementos centrais.

- Debater o papel dos intervenientes do sector da segurança na concepção e implementação de uma estratégia e política nacionais de segurança cibernética.

- Descrever princípios centrais, boas práticas e lições aprendidas durante a elaboração e implementação da estratégia e política nacional de segurança cibernética.

ENQUADRAMENTO:

Em muitos aspectos, as estratégias de cibersegurança estão no centro dos esforços nacionais para responder aos desafios cibernéticos. As estratégias nacionais de cibersegurança são necessárias para definir e dar prioridade às principais ameaças, que variam significativamente de país para país e de região para região. Juntamente com a legislação, as estratégias nacionais são os principais veículos através dos quais são atribuídos papéis e responsabilidades intergovernamentais para a segurança do ciberespaço. Podem também ser utilizadas como instrumentos para assegurar que a cibersegurança seja dotada de recursos adequados e para monitorizar o progresso dos esforços nacionais de defesa contra as ameaças cibernéticas. Se actualizadas com regularidade, as estratégias de segurança cibernética podem assegurar que os esforços nacionais de segurança do ciberespaço respondam e se adaptem a um ambiente de ameaças em mudança.

Como em qualquer estratégia relacionada com a segurança, o processo através do qual a estratégia é formulada é tão importante quanto o seu conteúdo. É necessária uma adesão e apoio políticos de alto nível para resolver conflitos entre diferentes agências e ministérios, bem como assegurar uma comunicação clara e sistemática com o público. Com um processo claro para dar prioridade às ameaças, as estratégias nacionais podem ser ferramentas úteis para gerir escassos recursos governamentais e encaminhar o apoio externo para os locais onde ele for mais necessário. As estratégias que são o produto de consultas com uma vasta gama de governos, a sociedade civil e as partes interessadas externas podem conseguir uma ampla adesão, melhorando a coordenação governamental e catalisando os esforços nacionais para enfrentar os principais desafios de segurança.[8] Estas considerações são particularmente cruciais num contexto africano, onde os governos dependem frequentemente do apoio dos intervenientes externos e onde o envolvimento das várias partes interessadas é crucial para assegurar a responsabilização, a inclusão e o respeito pela segurança dos cidadãos.

Infelizmente, a maioria dos governos africanos ainda não desenvolveu uma estratégia nacional de cibersegurança De acordo com os dados mais recentes disponíveis da União das Tecnologias de Informação das Nações Unidas, apenas 16 dos 54 países africanos completaram estratégias nacionais de cibersegurança. As estratégias de outros quatro países - Tunísia, Botswana, Gana, e

[8] Consulte o conjunto de ferramentas de Centro África de Estudos Estratégicos, "Toolkit for National Security Strategy Development," 2021. 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

Zâmbia - permanecem em forma de projeto.[9] Mesmo em países onde a penetração da Internet é baixa, a falta de uma estratégia nacional de cibersegurança é uma oportunidade perdida para otimizar os benefícios e reduzir os riscos de uma digitalização crescente .

QUESTÕES PARA DEBATE:

- Para os países com uma estratégia nacional de cibersegurança, qual foi o processo através do qual a estratégia do seu país foi desenvolvida ou implementada? Para países sem uma estratégia nacional de cibersegurança em vigor, qual foi a sua experiência no que diz respeito ao desenvolvimento e implementação de estratégias e políticas sectoriais sobre questões cibernéticas?

- Que papel tem ou deverá ter o sector da segurança no processo de elaboração de uma estratégia de segurança do ciberespaço?

- Que boas práticas, procedimentos, ou mecanismos de coordenação ou supervisão são necessários para garantir que os intervenientes da segurança nacional desempenham um papel produtivo na formulação de políticas e estratégias sobre as questões cibernéticas?

LEITURA RECOMENDADA:

International Telecommunication Union (ITU), *Guide to Developing a National Cybersecurity Strategy*, 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

Centro África de Estudos Estratégicos, 2021, "National Security Strategy Development Toolkit," (Desenvolvimento da Estratégias de Segurança Nacional em África) Section 1, pp. 1-9.
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 and Joel Amegboh, "Rethinking National Security Strategies in Africa," *International Relations and Diplomacy* 9 (01): 2021, 1-17.
http://www.davidpublisher.org/Public/uploads/Contribute/60a72058556ba.pdf

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

Federal Republic of Nigeria, *National Cybersecurity Strategy and Policy,* fevereiro 2021.
https://www.cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf

[9] Consultar o Repositório de Estratégia de Cibersegurança da UIT: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

Claudia Almeida et al., "Problemática da Cibersegurança: o Caso da Estratégia Nacional de Segurança no Ciberespaço," *Informação e Segurança no Ciberespaço,* setembro 2018. https://www.researchgate.net/publication/327515395_A_Problematica_da_Ciberseguranca_o_Caso_da_Estrategia_Nacional_de_Seguranca_no_Ciberespaco