CARTA INTERNACIONAL
ASSOCIAÇÃO BRASILEIRA DE RELAÇÕES INTERNACIONAIS

ISSN 2526-9038

Segurança cibernética em Moçambique: conceitos, infraestrutura e desafios de implementação

Cybersecurity in Mozambique: concepts, infrastructure, and implementation challenges

Seguridad cibernética en Mozambique: Conceptos, infraestructura y retos de aplicación

DOI: 10.21530/ci.v16n3.2021.1130

Marco Aurélio Chaves Cepik[1]
Henriques Manuel Marcelino[2]

Copyright:

• This is an open-access article distributed under the terms of a Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided that the original author and source are credited.

• Este é um artigo publicado em acesso aberto e distribuído sob os termos da Licença de Atribuição Creative Commons, que permite uso irrestrito, distribuição e reprodução em qualquer meio, desde que o autor e a fonte originais sejam creditados.

Resumo

Em 2018, Moçambique tornou-se signatário da *Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais*. O país participa também da União Internacional de Telecomunicações (ITU) e da Comunidade de Desenvolvimento da África Austral (SADC). Processos de securitização do ciberespaço em Moçambique constituem um mecanismo social que produz consequências materiais. Este artigo busca contribuir para a compreensão dos desafios de segurança cibernética de duas formas. Primeiro, explicitando conceitos como ciberespaço, internet, infraestrutura, segurança e defesa no âmbito digital. Segundo,

1 Professor titular do Departamento de Economia e Relações Internacionais (DERI) da Universidade Federal do Rio Grande do Sul (UFRGS), Rio Grande do Sul, Brasil. Doutor em Ciência Política (IUPERJ-UCAM). (mcepik@gmail.com). **ORCID: http://orcid.org/0000-0003-4147-5486**

2 Docente na Universidade Joaquim Chissano. Doutor em Estudos Estratégicos Internacionais (PPGEEI-UFRGS). (kgudja@gmail.com). **ORCID: https://orcid.org/0000-0002-9543-3022**

Artigo submetido em 01/10/2020 e aprovado em 05/04/2021.

propondo um modelo de maturidade adaptado para monitorar e avaliar o desenvolvimento da segurança cibernética em Moçambique.

Palavras-chave: Cibersegurança; Estratégia; Infraestrutura Crítica; Moçambique.

Abstract

In 2018, Mozambique became a signatory to the *African Union Convention on Cyber Security and Personal Data Protection*. The country also participates in the International Telecommunications Union (ITU) and the Southern African Development Community (SADC). Securitization moves related to the Mozambican cyberspace constitute a social mechanism with material consequences. This article seeks to contribute for the cyber security debate in two ways. First, offering clear definitions of concepts such as cyberspace, internet, infrastructure, security, and defense in the digital realm. Second, adapting existing cyber capabilities maturity models to assess the evolution of cybersecurity in Mozambique.

Keywords: Cybersecurity; Strategy; Critical Infrastructure; Mozambique.

Resumen

En 2018, Mozambique se convirtió en signatario de la Convención de la Unión Africana sobre la seguridad cibernética y la protección de los datos personales. El país también participa de la Unión Internacional de Telecomunicaciones (UIT) y de la Comunidad del África Meridional para el Desarrollo (SADC). Procesos de securitización del ciberespacio en Mozambique constituyen un mecanismo social que produce consecuencias materiales. Este artículo intenta contribuir de dos maneras para los debates sobre seguridad em el ciberespacio. Primero, aclarando conceptos como ciberespacio, Internet, infraestructura, seguridad y defensa en el ámbito digital. Segundo, adaptando un modelo de madurez para evaluar el desarrollo de la seguridad cibernética en Mozambique.

Palabras-clave: Ciberseguridad; Estrategia; Infraestructura Crítica; Mozambique.

Introdução[3]

Este artigo busca contribuir para o debate sobre o tema da cibersegurança de dois modos. Primeiro, explicitando o entendimento dos conceitos de ciberespaço, internet, segurança e defesa. Tal clarificação crítica é necessária para a análise da ~~a~~efetividade e da legitimidade das políticas públicas. Segundo, realizando um estudo de caso sobre desafios de segurança cibernética em Moçambique. Tais desafios serão discutidos tendo como referência os cinco pilares (legal, técnico, organizacional, construção de capacidades e cooperação) do *Global Cybersecurity Index* (ITU 2018a). Embora focado no caso de Moçambique, os problemas de segurança cibernética discutidos aqui são relevantes para toda a área de Relações Internacionais (Lu 2020; GCSCC 2016).

Antes de avançar, destacamos algumas informações preliminares sobre a digitalização em Moçambique. Em dezembro de 2019, o país contava com 6.523.613 usuários de internet. Cerca de 20,9% de uma população total de mais de 30 milhões (Internet World Stats 2020). A maioria dos usuários no país acessa a internet por meio de telefonia celular, como ocorre em outros países do Sul Global. Segundo o Instituto Nacional de Estatísticas (INE), em dezembro de 2018, havia 14 milhões de assinantes de telefonia móvel no país (Moçambique INE 2019). Com o agravamento da pandemia de Covid-19 e as necessidades de distanciamento físico entre as pessoas, a tendência tem sido de aumento do tráfego de internet, do número de assinantes de telefonia celular, bem como de provedores e usuários de plataformas. O adensamento digital traz oportunidades de desenvolvimento, mas também vulnerabilidades do e no ciberespaço.

Em 2018, Moçambique registrou mais de 1,5 milhão de ataques por mês. Mais de 90% foram ataques não-direcionados, principalmente *phishing*, *spam* e *malware* (vírus, *worms*, *trojans* e *bots*). Mas órgãos governamentais e universidades sofreram ataques tipo DDoS (negação de serviços) e *web defacement*. Em 2019 e 2020, além do aumento de ataques não-direcionados, foram detectados ataques persistentes, incluindo *ransomware*, *spyware* e quebras de chaves criptográficas, em redes governamentais, empresas e no sistema financeiro (Moçambique INAGE 2020c).

3 Os autores agradecem ao Conselho Nacional de Desenvolvimento Científico e Tecnológico do Brasil (CNPq) e ao Fundo Nacional de Investigação (FNI) de Moçambique, que tornaram possível o desenvolvimento deste artigo. Os autores também agradecem a Manuella Gadegast e Francisco Fabris, assistentes de pesquisa, bem como aos pareceristas e à equipe editorial de Carta Internacional.

Como destacou Kshetri (2019), ataques cibernéticos causam bilhões de dólares de prejuízo para as economias africanas anualmente. Muitos ataques são originados em outros países, inclusive da própria África. Existe, portanto, a necessidade de cooperação multilateral e multisetorial para lidar com o problema (Broadhurst 2006). Em 2012, com apoio da União Europeia e da *International Telecommunication Union* (ITU), a *South African Development Community* (SADC) adotou um modelo legal harmonizado para a caracterização de crimes cibernéticos, no âmbito do projeto S*upport for Harmonization of the ICT Policies in Sub-Saharan Africa* (HIPSSA). Entretanto, em 2016, apenas 11 dos 54 países africanos possuíam leis contra crimes cibernéticos (African Union-Symantec 2016).

Moçambique assinou, em 2018, a *Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais* (AU 2014). No mesmo ano, o país obteve um escore de 0,158 no *Global Cybersecurity Index* (GSI), ocupando a posição número 26 entre 42 países da África e a posição 132 entre 175 países no mundo (ITU 2018a). Um dos indicadores que compõem o pilar organizacional do GSI é a existência de documentos formais de estratégia. O governo moçambicano divulgou, em 2016, uma minuta de Estratégia Nacional de Segurança Cibernética para o período 2017-2021 (UNIDIR 2018). No momento em que concluímos este artigo, o documento ainda não havia sido oficialmente adotado. Segundo o *Global Cyber Strategies Index* compilado pelo *Centre for Strategic International Studies* (CSIS) dos Estados Unidos, em 2019, Moçambique possuía regulações em apenas uma (comércio eletrônico) de sete áreas. As outras seis áreas seriam a segurança cibernética, a defesa cibernética, o conteúdo digital, a proteção de dados e privacidade, a infraestrutura crítica e os crimes cibernéticos (CSIS 2019).

Para analisar a segurança cibernética em Moçambique, o restante do artigo foi organizado em quatro seções, seguidas de uma conclusão. Primeiro, definiremos seis conceitos fundamentais (securitização, ciberespaço, internet, infraestrutura crítica, cibersegurança e ciberdefesa). Na seção seguinte, serão estabelecidos marcos históricos do desenvolvimento cibernético em Moçambique. Também destacaremos a importância de se mapear vulnerabilidades em infraestruturas críticas. Na sequência, a terceira seção discutirá os desafios atuais de Moçambique na área de cibersegurança. Finalmente, na quarta seção, apresentaremos os lineamentos de um modelo para a avaliação continuada das políticas públicas na área de cibersegurança.

Seis conceitos: uma clarificação necessária

Incidentes cibernéticos tendem a aumentar diante da ausência ou fragilidade de políticas de prevenção e controle. Tais incidentes causam prejuízos e insegurança. Por outro lado, quando organizações estatais e privadas desenvolvem políticas e ações para aumentar a segurança, elas também incorrem em custos de oportunidade e de transação, inclusive o risco de abusos e violações de direitos (Rid e Buchanan 2014). Isso ocorre por causa da dinâmica dos processos de securitização.

Segundo Guzzini (2011), a securitização de temas ou sujeitos sociais é um mecanismo de interação que envolve atos de fala e processos materiais. Nos termos da Escola de Copenhagen, trata-se do processo por meio do qual uma comunidade política constrói intersubjetivamente, de modo mais ou menos polêmico, uma compreensão comum de que algo ou alguém está ameaçando a existência de outro algo ou alguém (Buzan, Waever e De Wilde 1998). Quando um tema é securitizado, ele é alçado para fora do processamento político "normal" dos conflitos de interesse e opinião. Passa a ser tratado com medidas e recursos excepcionais (inclusive o segredo governamental), sob a justificativa de se tratar de ameaça existencial. Quando um ator, por exemplo, um governo, propõe que um determinado público ou conjunto de recursos seja securitizado, é preciso que outros atores políticos e societais reconheçam as ameaças à integridade física e subjetiva. Tais processos envolvem causas e efeitos materiais das construções intersubjetivas. Normativamente, o ideal é que as questões relevantes de uma sociedade sejam tratadas segundo regras comuns de adjudicação de conflitos. Ou seja, em termos normativos, o objetivo seria "(de)securitizar" a maior parte possível dos problemas (Reisdoerfer e Alcântara 2020).

Portanto, é preciso definir precisamente termos como ciberespaço, internet, infraestrutura crítica, cibersegurança e ciberdefesa.

O ciberespaço é o ambiente criado pelo uso da eletroeletrônica e do espectro eletromagnético, no qual ocorre a criação, armazenamento, processamento, transmissão de informações e comunicações em redes analógicas e digitais mais ou menos interconectadas (Kuehl 2009). Nesse sentido, Najah (2020) argumenta que o ciberespaço é formado pela união dos componentes físicos e virtuais. O autor define o ciberespaço como interação dinâmica entre três camadas. A primeira é a camada física, incluindo elementos materiais tais como satélites, cabos submarinos, *data centers*, telefonia fixa/móvel etc. A segunda camada é a das

aplicações, a qual inclui os sistemas operacionais, protocolos, códigos, aplicações, bases de dados etc. A camada virtual permite a utilização da infraestrutura física, mas também a produção e circulação de conteúdos produzidos. A terceira camada é chamada de cognitiva. Para o autor, é a camada individual e coletiva que reúne o universo das duas camadas anteriores, possibilitando assim que as informações sejam produzidas, redes sociais sejam criadas e discussões e trocas de dados ocorram em tempo real.

As conexões entre diversos dispositivos, tais como rádio, telefonia fixa/móvel e televisão por satélite, sistemas de controle de tráfego aéreo e navegação marítima, moldaram o ciberespaço ao longo do tempo (Canabarro e Borne 2013, 2). Com a evolução das comunicações mundiais e o avanço da digitalização, tornou-se comum falar de internet como sinônimo de ciberespaço. Na verdade, o ciberespaço é anterior ao surgimento da internet. Ou seja, quando novas tecnologias da Era Digital superarem a configuração atual da internet, o ciberespaço continuará existindo. Enquanto componente decisivo do ciberespaço, a internet pode ser definida como a estrutura internacional das redes de computadores digitais interligados via cabos submarinos, fibra ótica e satélites (Canabarro e Borne 2013). Conforme Leal (2015), a internet também se caracteriza pelo uso de protocolos comuns para as comunicações e aplicações, principalmente o TCP-IP (*Transmission Control Protocol – Internet Protocol*).

Outro conceito a ser explicitado é o de Infraestruturas Críticas. Esse conceito abarca os sistemas, serviços e funções de um país, cuja interrupção ou destruição debilitaria o provimento de energia, saúde, água, comida, transportes, comunicações, comércio e segurança nacional (ITU 2008). Os países diferem na percepção sobre quais são os componentes críticos da infraestrutura. Por exemplo, o Reino Unido categoriza as infraestruturas segundo sua criticidade e a probabilidade de impactos resultantes de vulnerabilidades e ameaças (United Kingdom 2020). A infraestrutura cibernética crítica, por exemplo, seria formada pelo conjunto de equipamentos, sistemas e serviços de informação e comunicação que permitem o funcionamento da internet e de outros componentes do ciberespaço (NICCS 2020).

Também é importante diferenciar conceitualmente segurança e defesa. Por segurança, entende-se uma condição de proteção relativa na qual um sujeito individual ou coletivo é capaz de neutralizar ameaças e violências discerníveis (Cepik 2001).

A definição adotada demanda três esclarecimentos adicionais. Primeiro, uma ameaça expressa (de modo verbal, gestual, sonoro ou visual) a intenção de causar dano, dor ou perda. Ou seja, uma ameaça crível é uma manifestação de poder, mediada por processos interpretativos e intersubjetivos. O segundo esclarecimento é que as ameaças tendem a estar relacionadas com vulnerabilidades percebidas, podendo ser existenciais ou menos extremas. O uso intencional de poder que resulta em ferimentos, mortes, dano psicológico, subdesenvolvimento ou privação constitui uma violência (WHO 2014, 84). Finalmente, vale destacar vulnerabilidades e ameaças que, de maneira articulada, constituem a insegurança (USA 2014).

A existência de vulnerabilidades e/ou ameaças afeta a segurança de diferentes atores no ciberespaço e do próprio ciberespaço. Assim, a segurança cibernética é obtida por meio de atividades e medidas preventivas, de redução de vulnerabilidades, bem como por meio de ações dissuasórias e/ou coercitivas, que visam a neutralizar ameaças e a proteger o espaço cibernético. Concretamente, trata-se da segurança dos desenvolvedores, provedores, usuários, infraestrutura, acervos informacionais e comunicações (ITU 2007). A segurança cibernética é um processo interativo e dinâmico, não um *datum* fixo no tempo e no espaço. Tal processo é capturado pelo conceito de securitização. Nem todas as vulnerabilidades do ciberespaço deveriam ser tratadas como problemas de segurança. A universalização do acesso, por exemplo, demanda medidas de inclusão digital que não podem ser implementadas por forças de segurança.

Assim como as políticas públicas de governança da internet e do ciberespaço são mais amplas do que as medidas de segurança, as políticas e estratégias de cibersegurança são mais amplas do que a defesa cibernética. Por defesa, entenda-se conceitualmente o conjunto de medidas ativas e passivas para proteger as capacidades do Estado e para neutralizar (dissuadir ou destruir) as forças inimigas engajadas em ameaças, ataques, interferências ou perigos não intencionais (USA 2020). As políticas de defesa cibernética são implementadas em três níveis (estratégico, operacional e tático) de preparação e condução da guerra cibernética (Springer 2017). Em parte, a confusão entre segurança e defesa cibernética ocorre porque as técnicas e ferramentas utilizadas nos ataques podem ser similares (*e.g.* extração de metadados, instalação de códigos maliciosos, negação de serviço, *backdoors*, corrupção de *software*, manipulação de *logs* e arquivos).

Porém, a confusão entre as duas coisas (segurança e defesa) pode ser mais ou menos deliberada. Como acontece quando o ativismo cibernético, o crime, a insegurança e os atos de guerra são tratados como um contínuo, por exemplo, por parte de governos ou grupos de interesses. Indivíduos, grupos criminosos, ou mesmo terroristas não possuem as mesmas capacidades operacionais que grandes empresas privadas e governos. Atores não estatais podem conduzir operações cibernéticas ofensivas e defensivas, mas dificilmente poderão se equiparar ou produzir a combinação de efeitos lógicos e cinéticos que caracteriza a defesa cibernética (Cepik, Canabarro e Ferreira 2015). Cada país conceitua a ciberdefesa de acordo com os seus objetivos e interesses nacionais, mas é preciso cuidado com as diferenças entre defesa e segurança (IISS 2020).

A utilização imprecisa de termos como "ciber conflito", "segurança cibernética" ou "guerra cibernética", segundo Choucri (2012, 19), indica usos não consolidados que levam a respostas inconsistentes. Diferenciar as ameaças de segurança dos atos de guerra, embora difícil em casos mais extremos, é um passo necessário para o dimensionamento e a organização dos esforços governamentais em cada setor. Com base nos conceitos discutidos até aqui, mas também nos objetivos de segurança cibernética apresentados em documentos da SADC, União Africana e ITU, passamos, a seguir, a discutir o caso de Moçambique na África Austral.

O ciberespaço moçambicano

A evolução do ciberespaço moçambicano começou em 1933, com a primeira emissão analógica do Rádio Clube de Moçambique, ainda sob a dominação colonial portuguesa. Em 1981, o governo da República Popular criou a Televisão Experimental de Moçambique, que inicialmente transmitia apenas aos domingos para a região de Maputo. Atualmente chamada de TVM, a emissora pertence ao governo nacional. Desde 2001, transmite para 80% do território do país via satélite e, mais recentemente, tornou-se acessível via internet. Na década de 2000, desenvolveu-se a digitalização da rádio e da televisão no país, tanto via cabo quanto via satélite, com operadoras estatais e privadas (Miguel 2015).

Além do segmento de comunicações, o espaço cibernético moçambicano também foi conformado pela evolução da computação e da internet. Segundo Kluzer (1993), o primeiro computador foi instalado em 1964, numa fábrica de tabaco. Posteriormente, a computação foi utilizada para a estatística ferro-portuária

nos Armazéns Gerais dos Caminhos de Ferro de Moçambique (CFM). Conforme relata Chamango (2012), o uso de computadores para cálculos na educação superior desenvolveu-se a partir do Centro de Informática da Universidade Eduardo Mondlane, fundada em 1976, logo depois da independência. Em 1987, um decreto presidencial criou a Comissão Especial de Informática, permitindo o surgimento das primeiras empresas do setor (Matusse 2003).

Em 1993, depois da promulgação da nova Constituição (1990) e do Acordo Geral de Paz (1992), Moçambique foi o terceiro país africano a conectar-se com a rede mundial de computadores. África do Sul e Egito foram os primeiros a participarem da internet na África. Por meio da SADC, o governo moçambicano passou a cooperar com outros países, como a Tanzânia, nas áreas de formação acadêmica e assistência técnica em Tecnologias de Informação e Comunicação (TIC). Segundo Muchanga (2006), o desenvolvimento da infraestrutura de redes foi lento no país.

Em dezembro de 2000, o Conselho de Ministros aprovou o texto da primeira Política de Informática, que registrava à época a existência de 11.516 computadores no país, mais da metade deles em Maputo (Moçambique INTIC 2000). Com uma demanda crescente por computadores, em 2009, em parceria com a empresa multinacional Sahara, sediada em Joanesburgo, iniciou-se em Moçambique a produção de microcomputadores da marca Dzowo. Embora não seja mais fabricado, o Dzowo foi importante para a configuração do ciberespaço moçambicano. Em 2018, segundo dados do Instituto Nacional de Comunicações (INCM), o país possuía 42 provedores de acesso à internet, com 6.182.217 computadores conectados (Moçambique INCM 2018).

A espinha dorsal (*backbone*) da internet em Moçambique é formada por uma Rede Nacional de Transmissão em banda larga cobrindo as sedes dos 128 distritos do país. O maior provedor de acesso banda larga é a empresa estatal Telecomunicações de Moçambique (TDM). Redes privadas são operadas também pelas empresas Vodacom e Movitel. Em nível regional e internacional, o país está conectado via cabos submarinos da SEACOM e do *Eastern Africa Submarine Cable System* (EASSy), ambos com *landing points* em Maputo. A transmissão até as sedes distritais é feita por meio de sistemas de microondas ponto a ponto em lugares de difícil acesso. Também são utilizados serviços de *very-small-aperture terminal* (VSAT) para acesso à internet e comunicações via satélite (Moçambique TDM, 2020d).

Como destaca Kizza (2020), vulnerabilidades cibernéticas são agravadas por fragilidades na governança de equipamentos, redes, sistemas, ativos informacionais e pessoas que desenvolvem e utilizam os recursos cibernéticos. Para Marcelino (2014), a obsolescência tecnológica de parte da infraestrutura, a escassez de pessoal com conhecimento técnico especializado e a ausência de políticas, doutrinas e regras de gestão de riscos e resposta a incidentes dificultam o amadurecimento da segurança cibernética no país. Em 2015, foi criado o primeiro centro nacional de resposta a emergências cibernéticas, chamado CERT-MZ, subordinado ao MCTESTP. Entretanto, em setembro de 2020, a equipe do centro era formada por apenas seis especialistas (Moçambique CERT-MZ 2020b).

Atualmente, a governança do ciberespaço moçambicano é dividida entre dois órgãos principais. O Instituto Nacional das Comunicações de Moçambique (INCM), vinculado ao Ministério dos Transportes e Comunicações (MTC), regula o acesso, a interligação e a interoperabilidade das redes dos diferentes operadores. Por sua vez, o Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC), subordinado ao Ministério da Ciência e Tecnologia, Ensino Superior e Técnico-Profissional (MCTESTP), é responsável pelo regime jurídico das transações eletrônicas e do comércio digital. A implementação da Rede Electrónica do Governo (GovNET) e prestação de serviços digitais, anteriormente sob a responsabilidade do INTIC, passaram para a alçada do Instituto Nacional de Governo Electrónico (INAGE). Criado em dezembro de 2017, o INAGE também é subordinado ao MCTESTP. Dentre as atribuições do órgão, se inclui a de garantir a segurança cibernética dos recursos de TI do governo central e dos governos provinciais.

Conforme Zaballos e Jeun (2016), nos países em desenvolvimento, os prejuízos causados pelos incidentes cibernéticos são difíceis de estimar por falta de mapeamento e proteção das infraestruturas críticas (IC). A proposta inicial de Estratégia Nacional de Cibersegurança, apresentada pelo governo moçambicano em 2016, mesmo definindo como um dos seus objetivos a proteção da infraestrutura informacional, não apresentava critérios para a classificação das infraestruturas em termos de sua criticidade e vulnerabilidade diante de incidentes, crimes e ataques militares.

Para o caso de Moçambique, poderiam ser adaptadas as metodologias já desenvolvidas pela União Europeia e África do Sul, as quais, por sua vez, foram moldadas segundo as diretrizes da ITU. No caso da metodologia europeia, por exemplo, as infraestruturas são agrupadas por afinidades funcionais e a criticidade é avaliada conforme os impactos sofridos afetem um ou mais setores simultaneamente

(Ferreira 2016). No caso sul-africano, sistemas e ativos informacionais dos setores militar, policial, de saúde, água, comunicações, transporte, energia e finanças são considerados críticos (South Africa 2019).

Um exemplo de infraestrutura crítica em Moçambique é o sistema de geração e transmissão de energia hidroelétrica de Cahora Bassa. Situada no Rio Zambeze, na região central de Moçambique, o lago artificial da represa é o quarto maior da África (depois de Assuã, Volta e Kariba), com uma extensão de 2.700 km². A vazão de água passa por cinco turbinas que geram mais de 2.000 megawatts, utilizados para prover energia para Moçambique (250 MW), África do Sul (1.100 MW) e zimbabué (400 MW), além de Malawi e Zâmbia. Maior complexo hidroelétrico da África Austral, a energia de Cahora Bassa alimenta mais de 70% da rede elétrica de Moçambique. Além da represa e da usina geradora, fazem parte do complexo mais de 1.420 km de linhas de alta tensão que transmitem energia para vários centros de redistribuição em toda a região (ALER 2017). A crescente digitalização dos sistemas de gestão da rede elétrica (*digital electric grid*) aumenta a eficiência e reduz os custos de geração e distribuição. Mas, por outro lado, cria vulnerabilidades cibernéticas devido ao uso de arquiteturas de controle do tipo *supervisory control and data acquisition* (SCADA). No caso de uma interrupção de serviços ou destruição física causada por uma combinação de ataques cibernéticos e sabotagem, a perda de Cahora Bassa não poderia ser compensada por nenhuma combinação de outras infraestruturas do setor, tais como a Central Termoeléctrica a gás em Ressano Garcia, ou a barragem de Mphanda Nkuwa, na província de Tete, com capacidade de geração de 1.500 megawatts (Moçambique INE 2019).

Como não existem avaliações sistemáticas de risco cibernético no país, é difícil estimar a probabilidade de ocorrência de ataques catastróficos, mesmo diante da altíssima criticidade da infraestrutura. Vale lembrar, porém, que, entre 1985 e 1997, Cahora Bassa ficou paralisada por causa da guerra civil em Moçambique. Vale notar, ainda, que, em 2020, ocorreram diversas explosões suspeitas no Irã, duas delas em usinas de geração de energia elétrica nas províncias de Khuzestan e Isfahan, possivelmente envolvendo ataques cibernéticos (Bryen 2020).

Ou seja, o mapeamento das infraestruturas críticas é um desafio para a implementação de uma Estratégia de Segurança Cibernética em Moçambique. Na próxima seção, discutiremos alguns desafios adicionais que nos parecem relevantes.

Desafios de segurança cibernética em Moçambique

Os desafios de segurança cibernética em Moçambique podem ser sintetizados tendo como referência o *Global Cybersecurity Index* (GCI). Como se sabe, os 25 indicadores a partir dos quais é calculado o índice são classificados em cinco categorias ou pilares: legal, técnico, organizacional, capacidades e cooperação (ITU 2018a, 8).

No âmbito legal, o país vem adotando instrumentos relevantes na área digital (Moçambique 2020a). Vale citar, por exemplo, a Lei de Transacções Electrónicas (03/2017), a nova Lei das Telecomunicações (04/2016), a Lei da Revisão do Código Penal (35/2014), que incluiu o título III sobre os crimes informáticos e fraudes eletrônicas, o Decreto do Registo de Cartões SIM (18/2015), além do Decreto sobre a Interoperabilidade do Governo Eletrónico (67/2017). Destaca-se também a Política para a Sociedade da Informação (Resolução 17 do Conselho de Ministros 2018). Em 2019, a política foi desdobrada em um Plano Estratégico (2019-2028) e um Plano Operacional (2019-2023) para a construção da Sociedade da Informação em Moçambique. Em relação à segurança cibernética, porém, permanecem dois desafios. O primeiro é internalizar, por meio de ratificação pela Assembleia Nacional, as convenções e acordos internacionais assinados pelo governo no âmbito da SADC, União Africana e ITU. O segundo desafio é adaptar a legislação à evolução das tecnologias e da geopolítica global. Tecnologias associadas ao 5G e à Inteligência Artificial, por exemplo, tendem a modificar rapidamente o mercado e o contexto político.

Das seis medidas técnicas avaliadas pela ITU, Moçambique encontra-se mais atrasado em duas. A primeira seria na criação de um Centro Nacional de Governança Cibernética, responsável pela coordenação estratégica do CERT-MZ na construção da rede moçambicana de *Computer Security Incident Response Teams* (CSIRTs) atuando em organizações públicas e privadas. A designação de um *locus* responsável e de padrões de atuação nos parece uma condição para as demais medidas técnicas. A segunda medida técnica envolve a definição e implementação de padrões e procedimentos para a proteção de acervos informacionais, conexões remotas às redes via *proxy*, soluções seguras de *cloud computing*, proteção contra *software* malicioso e medidas para melhorar a capacidade de atribuição de responsabilidades (técnicas e políticas) pelos ataques (Romanosky e Boudreaux 2020, 04). A minuta da estratégia divulgada em 2016 não especifica autoridade,

métricas, critérios, indicadores, periodicidade e procedimentos para a avaliação das diretrizes gerais de cibersegurança.

No âmbito organizacional, os desafios de segurança cibernética em Moçambique estão conectados aos desafios técnicos. O mais crítico deles é a adoção oficial de uma Estratégia Nacional de Cibersegurança. Mais do que uma formalidade, um documento de estratégia sinaliza objetivos, compromissos e meios. Segundo o guia da ITU para a elaboração de documentos nacionais de cibersegurança, seria necessário indicar ou criar uma agência única responsável pelo tema (ITU 2018b). Atualmente, em Moçambique, a responsabilidade pela segurança do ciberespaço é partilhada de maneira pouco precisa entre o INCM, o INTIC, o INAGE, o Ministério da Defesa Nacional (MDN) e o Ministério da Educação e Desenvolvimento Humano (MINED).

O quarto desafio é a construção de capacidades humanas. Em Moçambique, as ações governamentais nessa área se concentram em campanhas de conscientização e cursos sobre segurança cibernética para estudantes universitários de Ciência da Computação e Engenharia. Mas a escassez de pessoal qualificado para atuar em empresas e órgãos públicos é uma vulnerabilidade em toda a região. Segundo o relatório *Cyber Security Skills Gap* publicado pela empresa Serianu, em 2018, havia 1.700 profissionais habilitados em segurança cibernética atuando no Quênia, o país com o segundo GCI mais elevado da África (Serianu 2018). Um desafio para Moçambique é aumentar o número de profissionais certificados em áreas como *cloud security*, análise forense, prevenção de perdas, manejo de incidentes e avaliação de risco.

O quinto desafio de Moçambique é aumentar a cooperação internacional em cibersegurança, especialmente no âmbito da SADC e da União Africana. Há custos elevados e interesses empresariais e políticos envolvidos em quaisquer esforços de cooperação. Ainda mais em áreas caracterizadas por incerteza, assimetria informacional e ganhos relativos. Por outro lado, para garantir a estabilidade do ciberespaço, é necessário cooperar para proteger a infraestrutura crítica compartilhada, para garantir a integridade das transações *online* e para proteger os dados dos usuários e dos provedores (públicos e privados).

Ademais, os custos da cooperação e das ações de segurança também precisam ser ponderados em relação aos prejuízos gerados pela falta de cooperação. Em 2017, os prejuízos causados por incidentes, crimes e ataques cibernéticos foram estimados em 3,5 bilhões de dólares americanos no continente africano

(Mathe 2019). Segundo Kshetri (2019), somente os crimes cibernéticos custaram, em 2018, aos países africanos o equivalente a 2,7 bilhões de dólares americanos, com destaque para Nigéria (649 milhões), Quênia (210 milhões), África do Sul (157 milhões) e Tanzânia (99 milhões). Segundo uma estimativa, em resposta, os investimentos em cibersegurança na África subiriam de 1,5 bilhão de euros, em 2017, para mais de 2,2 bilhões de euros em 2020 (Orange 2020). Seja como for, valores agregados incluem grandes discrepâncias. Segundo uma projeção, em 2020, a África do Sul investiria 933 milhões de dólares em cibersegurança, enquanto, no mesmo ano, as Ilhas Maurício investiriam um milhão (Frost e Sullivan 2018). Para efeito de comparação, o orçamento da SADC para a avaliação de riscos e a harmonização de regras de cibersegurança foi de 220,6 mil dólares em 2018.

A crise da Covid-19 também está alterando as prioridades e os orçamentos das empresas e governos na área de cibersegurança. Segundo um relatório da consultoria McKinsey, de julho de 2020, os cerca de 250 *Chief Information Security Officers* (CISOs) que responderam a um questionário da empresa relataram reorientação de esforços para a resposta a ataques de tipo *spear-phishing* e manipulação de engenharia social para espalhar pânico e desinformação entre a força de trabalho. Outras áreas que passaram a demandar mais esforços foram as de autenticação multifatores (MFA), redes privativas virtuais (VPN) e aplicações seguras para trabalho remoto (Anant, Caso e Schwarz 2020).

Em resumo, os desafios da cibersegurança em Moçambique podem ser sintetizados como um problema de institucionalização em três níveis (Ducheine 2014; Vedder et al. 2019). O primeiro é o nível político, onde os desafios legais, orçamentários e de cooperação encontram o *locus* mais adequado para serem resolvidos. Esse nível precisaria ser coordenado diretamente pela Presidência da República ou pelo gabinete do Primeiro Ministro. O segundo nível é o estratégico, no qual seriam enfrentados os desafios organizacionais e técnicos. A oficialização da Estratégia de Segurança Cibernética e a eventual criação de um Centro Nacional de Governança Cibernética seriam um marco crucial de institucionalização nesse plano. O terceiro nível é o tático-operacional. Nele, se desdobram tarefas mais especializadas, tais como políticas de e-governo ou defesa cibernética.

O estudo comparado da governança segura do ciberespaço pode ser feito tanto entre países, organizações e regiões, quanto em relação a diferentes momentos históricos considerando-se a trajetória de um mesmo ator, no caso, o país Moçambique. A seguir, discutimos criticamente uma das ferramentas

analíticas utilizadas internacionalmente para o monitoramento da evolução da segurança cibernética.

Um modelo de maturidade revisado

Modelos de maturidade podem ser definidos como conjuntos de características, atributos, indicadores ou padrões que permitem monitorar a progressão das capacidades em diferentes áreas e disciplinas (USA 2014, 02). Além do monitoramento, um modelo de maturidade também pode ser utilizado como guia para a implementação e avaliação dos processos e políticas de melhoria em uma organização (Rocha 2000). Embora sejam bastante utilizados nas áreas de Engenharia de Produção e Administração, modelos de maturidade tendem a idealizar algum "ponto de chegada", frequentemente definido com referência (*benchmark*) às experiências de países e/ou organizações mais ricas e poderosas. Constrangimentos estruturais e outros fatores de reprodução de desigualdades precisariam ser mobilizados para explicar diferenças persistentes no tempo e no espaço. Em outras palavras, modelos descrevem, enquanto teorias explicam. A continuidade da pesquisa sobre a segurança cibernética em Moçambique precisará de esforços teóricos e empíricos que expliquem as causas e consequências dos processos de securitização nesse domínio da atividade naquele país. Não obstante, tendo consciência das limitações e vieses, a utilização de algum modelo de maturidade ajuda a descrever (monitorar) as políticas de segurança cibernética desenvolvidas pelo governo moçambicano e pelos demais atores ao longo do tempo. Ainda assim, resta saber qual modelo utilizar.

Na área de segurança cibernética, destacam-se dois modelos de maturidade bastante utilizados internacionalmente. O primeiro é o Modelo de Maturidade de Capacidade de Cibersegurança para Nações (*Cybersecurity Capacity Maturity Model for Nations* – CMM), desenvolvido pelo Centro Global de Capacidades de Segurança Cibernética (*Global Cyber Security Capability Centre – GCSCC*) da Universidade de Oxford (GCSCC 2016). O segundo é o Modelo de Maturidade de Capacidade de Cibersegurança (*Cybersecurity Capability Maturity Model* – C2M2), desenvolvido pelos Departamentos de Energia (DOE) e de Segurança Interna (DHS) dos Estados Unidos da América (USA 2014). Vamos descrever brevemente ambos a seguir.

Começamos pelo CMM, desenvolvido para orientar o desenvolvimento da segurança cibernética em âmbito nacional. Na edição revisada de 2016, o modelo de Oxford trabalha com cinco dimensões: D1 – Política e estratégia (*Cybersecurity Policy and Strategy*). D2 – Cultura e Sociedade (*Cyber Culture and Society*). D3 – Educação, treinamento e habilidades (*Cybersecurity Education, Training and Skills*). D4 – Modelos regulatórios e legais (*Legal and Regulatory Frameworks*). D5 – Padrões, organizações e tecnologias (*Standards, Organisations, and Technology*).

Cada dimensão é subdividida em fatores. Assim, por exemplo, a primeira dimensão, Política e Estratégia de Segurança Cibernética (*Cybersecurity Policy and Strategy*), divide-se em seis fatores: D1.1 – Estratégia Nacional de Segurança (*National Security Strategy*). D1.2 – Resposta a Incidentes (*Incident Response*). D1.3 – Proteção de Infraestrutura Crítica (*Critical Infrastructure Protection*). D1.4 – Gerenciamento de Crises (*Crisis Management*). D1.5 – Considerações de Defesa Cibernética (*Cyber Defence Consideration*). D1.6 – Redundância de Comunicações (*Communications Redundancy*). As outras quatro dimensões também são subdivididas em fatores, gerando um total de 52 linhas na matriz. O modelo de Oxford representa a ideia de amadurecimento dividindo cada "linha" em cinco colunas, representando os estágios de amadurecimento. Tais estágios são classificados em ordem crescente, como *start-up*, *formative*, *established*, *strategic* e *dynamic*. Com uma matriz 52x5, o modelo de maturidade de Oxford já seria bastante complexo, supondo o preenchimento de 260 células com informações qualitativas. Mas o CMM prevê ainda que se observe indicadores distintos (entre um e cinco) para cada fator em cada estágio. Com isso, sobe para 600 o número total de células na matriz (GCSCC 2016, 13-57).

No caso do C2M2, o modelo estadunidense foi desenvolvido para acompanhar e guiar o processo de institucionalização das práticas e capacidades de segurança cibernéticas em organizações de diferentes tamanhos e graus de complexidade, não de países como um todo. O modelo C2M2 foi desenvolvido em conjunto pela Carnegie Mellon University e pelo Departamento de Energia (DOE) com a participação de especialistas do governo e da iniciativa privada. Assim como no caso do CMM, o modelo C2M2 considera dimensões, chamadas de domínios.

A arquitetura do modelo C2M2 considera dez domínios: D1 – Gerenciamento de risco (*Risk Management*). D2 – Ativos, mudança e configuração do gerenciamento (*Asset, Change, and Configuration Management*). D3 – Identidade

e gerenciamento de acessos (*Identity and Access Management*). D4 – Ameaças e gerenciamento de vulnerabilidades (*Threat and Vulnerability Management*). D5 – Consciência Situacional (*Situational Awareness*). D6 – Compartilhamento de informações e comunicações (*Information Sharing and Communications*). D7 – Eventos e resposta a incidentes, continuidade das operações (*Event and Incident Response, Continuity of Operations*). D8 – Cadeia de suprimentos e gerenciamento da dependência externa (*Supply Chain and External Dependencies Management*). D9 – Gerenciamento da força de trabalho (*Workforce Management*). D10 – Gerenciamento do programa de segurança cibernética (*Cybersecurity Program Management*).

Para cada dimensão, o C2M2 considera um ou mais objetivos substantivos (próprios daquela dimensão) e um objetivo gerencial que é similar e se repete em todos os domínios. Por exemplo, no caso do sétimo domínio (D7 – Eventos e resposta a incidentes, continuidade das operações), o modelo prevê cinco objetivos: 1 – Detectar eventos de cibersegurança (*Detect Cybersecurity Events*). 2 – Escalar eventos de cibersegurança e declarar incidentes (*Escalate Cybersecurity Events and Declare Incidents)*. 3 – Responder a incidentes e eventos de cibersegurança escalados (*Respond to Incidents and Escalated Cybersecurity Events*). 4 – Planejar a continuidade das operações (*Plan for Continuity*). 5 – Atividades de gerenciamento (*Management Activities*). Para cada dimensão, o modelo considera três níveis de maturidade dos indicadores (*maturity indicator levels* – MILs). Para cada objetivo, observam-se as práticas que seriam indicadoras do nível de maturidade no atingimento daquele objetivo. Assim, por exemplo, no caso do objetivo D7.1 (Detectar eventos de Cibersegurança), três práticas seriam indicadoras do MIL 1: a existência de uma pessoa ou ponto de contato para que se possa relatar um evento, o relato do evento detectado propriamente dito, e o registro e acompanhamento do relatório. Já no nível de maturidade MIL 3, práticas mais complexas devem ser observadas, tais como a análise de correlações entre diferentes eventos para a identificação de padrões e tendências. Ao cabo, resulta que o C2M2 demanda a observação e catalogação de 312 práticas para a avaliação da maturidade da cibersegurança de uma organização (USA 2014, 18-48).

Como vimos, para cada rodada de monitoramento, o CMM demanda a obtenção e o preenchimento (*input*) de 600 informações, observadas em escala nacional, distintas em uma matriz de dados. Por sua vez, cada rodada de monitoramento utilizando-se o C2M2, envolve a compilação e o registro de

informações sobre 312 práticas em cada organização analisada. Considerando a realidade atual de Moçambique, onde faltam profissionais especializados em segurança cibernética e as instituições de governança ainda são relativamente frágeis, modelos de monitoramento tão complexos e custosos, na prática, acabam inibindo o desenvolvimento de capacidades nacionais de monitoramento e avaliação de políticas. Nesse sentido, nos parece mais viável e produtivo que os atores interessados no monitoramento da segurança cibernética moçambicana, sejam agências governamentais, sejam entidades da sociedade civil, empresas ou organizações de pesquisa, procurem focar, pelo menos inicialmente, em poucas variáveis e indicadores.

Por exemplo, poderíamos considerar cada um dos cinco pilares da ITU (legal, técnico, organizacional, capacidades e cooperação) como se fosse uma "variável", ou seja, como algo que não estará constante no tempo. Cada variável, por sua vez, poderia ter a sua "maturidade" mensurada segundo uma escala ordinal de três níveis (baixo, médio e alto). Mesmo sem a granularidade observacional permitida por variáveis intervalares ou sem a simplicidade e clareza classificatória permitida por variáveis categóricas dicotômicas, a adoção de uma escala ordinal simples já permitiria a formulação de juízos de valor comparáveis (entre diferentes observadores), baseados em evidências, em diferentes momentos no tempo. Na(s) primeira(s) rodada(s), a matriz de dados resultante teria 15 células, ao invés das centenas exigidas pelos modelos CMM e C2M2. Ainda tendo em vista a factibilidade do modelo proposto, sugere-se que sejam selecionados inicialmente poucos indicadores para que se possa aferir a variância de cada variável. Por exemplo, no pilar/variável denominado "legal", um indicador a ser observado seria a existência ou não de um documento oficial chamado Estratégia de Segurança Cibernética. Tendo em vista a avaliação qualitativa preliminar que realizamos neste artigo sobre os desafios de desenvolvimento de políticas de cibersegurança em Moçambique, nos parece relevante e viável atribuir ainda níveis de criticidade para cada indicador. Também nesse caso, a escala poderia ser tricotômica (A como mais crítico e C como menos crítico). Desta forma, os 15 indicadores selecionados permitiriam não apenas o monitoramento da "maturação", mas também a ponderação dos esforços a serem alocados em diferentes pilares e mesmo entre diferentes estágios de maturidade. No Quadro 1, o leitor encontra uma síntese do modelo proposto.

Quadro 1: Modelo de Avaliação da Cibersegurança em Moçambique

Pilar	Baixa maturidade	Média maturidade	Alta maturidade
Legal	Decreto oficializando a Estratégia Nacional de Cibersegurança (A)	Lei de Crimes Cibernéticos e Proteção de Dados (B)	Atualização da Legislação para os parâmetros da Segunda Era Digital (C)
Técnico	Mapeamento das Normas Técnicas necessárias e da Infraestrutura Crítica (IC) do ponto de vista da Segurança Cibernética (B)	Formalização de padrões técnicos gerais para a proteção de redes e acervos informacionais (C)	Especificação de normas, padrões e procedimentos em áreas emergentes (5G, IoT, *cloud computing*, análise forense etc..) (A)
Organizacional	Implantação de um Centro Nacional de Segurança Cibernética (A)	Ampliação da rede CERT/CSIRT governamental em todas as províncias (C)	Fórum permanente de atores interessados governamentais, empresariais e da sociedade civil para a governança cibernética (B)
Capacidades	Programa Nacional de Conscientização e Treinamento Básico em Cibersegurança (C)	Certificar tecnicamente os profissionais que atuam nos CERT/CSIRT de Moçambique (A)	Programa nacional de formação de mestres e doutores em governança cibernética, sendo a segurança e defesa uma das áreas de especialização (B)
Cooperação	Ratificar a Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais (B)	Harmonizar a legislação moçambicana com as diretrizes do já encerrado projeto HIPSSA da AU e a Lei Modelo da SADC para crimes cibernéticos (C)	Implementar Programa ITU-AU-SADC para a melhoria do GCI de Moçambique (A)

Fonte: elaborado pelos autores (2020).

Dado o patamar do qual Moçambique parte, estima-se que algumas medidas que correspondem a um baixo grau de maturidade em modelos como o CMM e o C2M2 teriam grande impacto, dado o risco de que a sua não implementação comprometa as iniciativas correspondentes a outros estágios de maturidade. Em outros pilares, entretanto, as medidas de maior criticidade correspondem aos

estágios médio e alto da maturidade em cibersegurança. Trata-se, obviamente, de uma primeira aproximação, que visa a estimular a reflexão sobre como desenvolver práticas de monitoramento e avaliação de políticas de cibersegurança em contextos como o de Moçambique.

Conclusão

Diante da crise causada pela epidemia Covid-19, um dos desafios que o país enfrenta é conseguir expandir o ciberespaço moçambicano e aumentar equitativamente sua densidade digital, evitando, ao mesmo tempo, agravar a exclusão digital que pode retardar o desenvolvimento nacional.

Com um Índice de Desenvolvimento Humano (HDI) de 0,446, que o situa na posição 180 entre 189 países, o governo de Moçambique tem muitas demandas orçamentárias. O gasto público em saúde, educação e infraestrutura física, por exemplo, é claramente mais prioritário do que investir em cibersegurança. Além disso, emergências como a epidemia de AIDS, a catástrofe causada pelo ciclone Idai em 2019, o recrudescimento da insurgência do Ansar al-Sunna no norte do país, ou a própria Covid-19 dificultam o planejamento e a construção regular de capacidades estatais (Chingotuane, Muchanga e Filipe 2020).

Por outro lado, como procuramos demonstrar neste artigo, o adensamento digital vem ocorrendo de maneira acelerada também em Moçambique. A estabilidade e a segurança do ciberespaço são necessárias para que a digitalização possa contribuir para o desenvolvimento sustentável e inclusivo (Orji 2018). Como demonstram os casos da China e da Malásia, estratégias de erradicação da pobreza extrema, especialmente em áreas rurais, dependem fortemente da infraestrutura de acesso à internet, programas de inclusão digital e ferramentas de *e-commerce* para a comercialização de produtos e serviços das comunidades (Chen 2020).

Nesse sentido, foram identificadas cinco atividades prioritárias (críticas) para a melhoria da segurança cibernética no país. Duas são de natureza eminentemente política e legal. Esse é o caso da adoção oficial de um documento de Estratégia Nacional de Cibersegurança, bem como da ratificação da *Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais*. Outras duas iniciativas demandam recursos públicos e a cooperação com o setor privado. São elas a implementação de um Centro Nacional de Segurança Cibernética com

capacidade técnica mínima para diagnosticar e responder a incidentes, bem como a certificação de um número razoável de profissionais, principalmente na área de proteção das infraestruturas críticas. A quinta medida é diplomática. Moçambique precisa melhorar o seu *Global Cybersecurity Index* (GCI), tomando como meta aproximá-lo do Quênia em prazo razoável. No relatório de 2018, destaca-se no caso daquele país o avanço no quadro legal, mas principalmente a colaboração local entre múltiplos atores interessados, desde o governo e os provedores de serviços básicos (água e eletricidade) até operadoras de telecomunicações e universidades (ITU 2018a, 25). A melhoria do CGI moçambicano demanda, pois, a cooperação internacional com a SADC, a AU e a ITU por meio de um programa específico que apoie as quatro iniciativas anteriores.

A segurança cibernética é um conceito amplo e polêmico, que inclui, mas não se resume, a prevenção e punição de crimes cibernéticos ou as ferramentas ofensivas e defensivas da guerra cibernética (De, 2021, 18). Neste artigo, optamos por assentar o conceito na ideia de estabilidade do ciberespaço e de proteção da infraestrutura crítica. Pesquisas adicionais podem avaliar aspectos mais específicos, como a questão da defesa cibernética em Moçambique.

Referências

Associação Lusófona de Energias Renováveis (ALER). 2017. *Energias Renováveis em Moçambique – Relatório Nacional de Ponto de Situação*. 2a. Edição. Disponível em: https://www.aler-renovaveis.org/contents/lerpublication/aler_2017_oct_relatorio-nacional-ponto-situacao-renovaveis-em-mocambique.pdf. Acesso em: 28 de setembro de 2020.

African Union (AU). 2014. *African Union Convention on Cyber Security and Personal Data Protection*. Malabo – Guiné Equatorial

African Union (AU) & Symantec. 2016. *Cyber Crime & Cyber Security Trends in Africa*. Mountain View: Symantec Corporation.

Anant, V., Caso, J., & Schwarz, A. 2020. *COVID-19 Crisis shifts cybersecurity priorities and budgets*. McKinsey & Company.

Broadhurst, R. 2006. *Developments in the global law enforcement of cyber-crime*. Policing: International Journal of Police Strategies and Management, 29(3), 403. DOI: https://doi.org/10.1080/15614263.2018.1507890.

Bryen, S. 2020. *Rising cyberattacks threaten real-world war*. Asia Times. Disponível em: https://asiatimes.com/2020/06/rising-cyberattacks-threaten-real-world-war/. Acesso em: 20 de setembro de 2020.

Buzan, B., Waever, O. & De Wilde, J. 1998. *Security: A New Framework for Analysis.* Lynne Rienner – Colorado, EUA.

Canabarro, D. R. & Borne, T. 2013. *Ciberespaço e Internet: Implicações Conceituais para os Estudos de Segurança*. Divulgação Científica em Relações Internacionais, Mundorama.

Cepik, M., Canabarro, D., & Ferreira, T. 2015. *Cyberwar: Clausewitzian Enconter*s. Space & Defense – Journal of The Undiet States Air Force Academy. volume 8. número 1.

Cepik, M. 2001. *Segurança Nacional e Segurança Humana: Problemas Conceituais e Consequências Políticas*. Security and Defense Studies Review. Volume 1. Issue n. 1. p.01-19.

Chamango, F. 2012. *Assessing ICT Policy Development and the Implementation Process: The Case of Mozambique*. Study undertaken for UECA by Francisco Mabila Chamango. Addis Ababa, ECA.

Chen, Y. 2020. *Three keys to poverty exit: technology, transport and tourism*. China Daily Global. Disponível em: http://epaper.chinadaily.com.cn/a/202008/31/WS5f4c4e44a310d95bf733ec91.html. Acesso em: 31 de agosto de 2020.

Chingotuane, E. & Muchanga, G. & Filipe, J. 2020. *Desafios na Luta contra a Covid-19, e no combate contra a Junta Militar e o Terrorism*o. Security Brief, Ano 02, volume 01, número 04. Maputo, CEEI Universidade Joaquim Chissano.

Choucri, N. 2012. *Cyberpolitics in International Relations*. Cambridge, MA: MIT Press. Massachusetts Institute of Technology – London, England

Center for Strategic & International Studies (CSIS). 2019. *Cyber Regulation Index*. V2. Disponível em: https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/global-cyber-strategies-index. Acesso em: 10 de setembro de 2020.

De, S. 2021. Security Threat Analysis and Prevention towards Attack Strategies. Kumar, G., D. K. Saini and N. Cuong, eds. 2021. *Cyber Defense Mechanisms: Security, Privacy, and Challenges*. CRC Press, Boca Raton, Florida. p. 01-22.

Ducheine. 2014. *Legal framework for (military) cyber operations*. Netherlands Defence Academy and University of Amsterdam (ACIL).

Ferreira, H. J. D. (2016. *Identificação e Caracterização de Infraestruturas Críticas – uma Metodologia*. Departamento de Estudos de Pós-Graduados, CEM-C 2015/2016. Instituto Universitário Militar, Portugal.

Frost & Sullivan. 2018. *Digital Market Overview: South Africa*. HM Government, London, United Kingdom.

Global Cyber Security Capability Centre. (GCSCC). 2016. *Cyber Security Capacity Maturity Model for Nations (CMM)*. University of Oxford. Disponível em: https://cybilportal.org/tools/cybersecurity-capacity-maturity-model-for-nations-cmm-revised-edition/. Acesso em: 21 de setembro de 2020.

Guzzini, S. 2011. *Securitization as a causal mechanism*. Security Dialogue, 42 (4-5), 329-341. DOI: https://doi.org/10.1177/0967010611419000.

International Institute for Strategic Studies (IISS). 2020. *Military Balance Complete*. Munich Security Conference – Alemanha.

International Telecommunication Union (ITU). 2007. *Global Cybersecurity Agenda, Framework for International Cooperation in Cybersecurity*. Geneva, Switzerland.

International Telecommunication Union (ITU). 2008. *Global Cybersecurity Agenda, High-Level Experts Group – Global Strategic Report*. Place des Nations – Geneva, Switzerland.

International Telecommunication Union (ITU). 2018a. *Global Cybersecurity Index (GCI)*. Geneva, Switzerland.

International Telecommunication Union (ITU). 2018b. *Guide to Developing a National Cyber Security Strategy – Strategic Engagement in Cybersecurity*. Geneva, Switzerland.

Internet World Stats. 2020. *Usage and Population Statistic*s. Disponível em: https://www.internetworldstats.com/africa.htm#mz. Acesso em: 26 de setembro de 2020.

Kizza, J. 2020. *Guide To Computer Network Security*. Fifth edition. Springer, Cham, Switzerland.

Kluzer, S. 1993. *The Political economy of IT in Susaharian Africa: the diffusion of computers in Mozambique*. (Tese de doutorado). The London School of Economics and Political Science – London, England.

Kshetri, N. 2019. *Cybercrime and Cybersecurity in Africa*. South African Banking Risk Information Centre (SABRIC). DOI: https://doi.org/10.1080/1097198X.2019.1603527.

Kuehl, D. 2009. *Cyberpower and National Security*, Ed. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz. Center for Technology and National Security Policy, National Defense University, USA, p. 39-40.

Leal, M. 2015. *Guerra e Ciberespaço: uma Análise a partir do Meio Físico*. (Dissertação de mestrado). UFRGS, Porto Alegre.

Lu, C. 2020. *Forging Stability in Cyberspace*. Survival, 62:2, 125-136, DOI: 10.1080/00396338.2020.1739959.

Marcelino, H. 2014. Dimensão de Defesa e Segurança Cibernética – Caso de Moçambique". (Dissertação de mestrado). Instituto Superior de Estudos de Defesa "Armando Emílio Guebuza" – Maputo, Moçambique.

Matusse, R., 2003. História da Informática em Moçambique. Mozambique Acacia Advisory Committee Secretariat. Universidade Eduardo Mondlane, Maputo.

Mathe, A. 2019. The Misunderstood World of Cybersecurity in Africa. Disponível em: https://www.policycenter.ma/opinion/misunderstood-world-cybersecurity-africa#.X3XtSS9h0Wo. Acesso em 16 de agosto de 2020.

Miguel, J. 2015. Digitalização da Televisão em Moçambique: Estratégias, Políticas e Reconfigurações. Revista UNINTER de Comunicação Vol. 3 n4, pp. 84-105. Disponível em: https://www.uninter.com. Acesso em: 09 de fevereiro de 2019.

Moçambique, República de. 2000. Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC). Política Nacional de Informática. Disponível em: https://www.intic.gov.mz/. Acesso em 29 de setembro de 2020.

Moçambique, República de. 2018. Autoridade Reguladora das Comunicações de Moçambique (INCM). Disponível em: https://www.arecom.gov.mz/. Acesso em 29 de setembro de 2020.

Moçambique, República de. 2019. Instituto Nacional de Estatística (INE). Anuário Estatístico 2018. Disponível em: http://www.ine.gov.mz/estatisticas/publicacoes/anuario/nacionais/anuario-estatistico-2018.pdf/view. Acesso em 29 de setembro de 2020.

Moçambique, República de. 2020a. "Boletim da República – Primeira Série". Várias datas. Disponível em https://www.portaldogoverno.gov.mz/por/Governo/Legislacao/Boletins-da-Republica. Acesso em 15 de setembro de 2020.

Moçambique, República de. 2020b. Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores de Moçambique (CERT-MZ). Disponível em: http://www.cert.mz/. Acesso em: 26 de setembro de 2020.

Moçambique, República de. 2020c. Instituto Nacional de Governo Eletrônico (INAGE). Disponível em: https://www.inage.gov.mz/. Acesso em 29 de setembro de 2020.

Moçambique, República de. 2020d. Telecomunicações de Moçambique (TDM). Disponível em: http://196.28.224.21/portdm/quem_somos_v2.html. Acesso em: 26 de setembro de 2020.

Muchang, J. 2006. Internet em Moçambique. Centro de Informática Universidade Eduardo Mondlane (CIUEM) – Maputo, Moçambique.

Najah, R. 2020. Le cyberespace africain: un état des lieux. Disponível em: www.policycenter.ma/opinion/le-cyberespace-africain-un-etat-des-lieux#.X2BMHpNKjGI. Acesso em: 1 de junho de 2020.

National Initiative for Cybersecurity Careers and Studies (NICCS). 2020. Cybersecurity Glossary. Disponível em: https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary#C. Acesso em: 10 de setembro de 2020.

Orange. 2020. Signal in the Noise: A Cybersecurity Data Odyssey. Orange Cyberdefense – Nanterre, França.

Orji, U. J. 2018. The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?., Masaryk University Journal of Law and Technology, Vol. 12:2, Nigeria.

Reisdoerfer, B., & Alcântara, B. Alemanha como Líder na Determinação de Ameaças Cibernéticas na União Europeia?. Revista Carta Internacional, v. 15, n. 2, 2020, p. 163-189. DOI: 10.21530/ci.v15n2.2020.1063.Reisdoerfer

Rid, T., & Buchanan, B. 2014. Attributing Cyber Attacks. Journal of Strategic Studies, 38(1-2), 4-37. DOI: https://doi.org/10.1080/01402390.2014.977382.

Rocha, A. 2000. Influência da Maturidade da Função Sistema de Informação na Abordagem à Engenharia de Requisitos. (Tese de doutorado). Universidade do Minho, Braga.

Romanosky, S., & Boudreaux, B. 2020. Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government. International Journal of Intelligence and CounterIntelligence. DOI: 10.1080/08850607.2020.1783877.

Serianu. 2018. African Cyber Security Report: Kenya. Disponível em: https://www.serianu.com/annual-reports.html.Acesso em: 30 de julho de 2020.

South Africa, Republic of. 2019. Act No. 8: Critical Infrastructure Protection Act. Government Gazette, Volume 653, # 42866, pages 02-59.

Springer, P. J. 2017. Encyclopedia of Cyber Warfare. Santa Barbara: ABC-CLIO.

United Nations Institute for Disarmament Research (UNIDIR). 2018. Cyber Policy Portal. Disponível em: https://unidir.org/cpp/en/. Acesso em: 27 de março de 2020.

United Kingdom. 2020. The national infrastructure. Disponível em: https://www.cpni.gov.uk/critical-national-infrastructure. Acesso em: 27 de março de 2020.

United States of America (USA). 2014. Cybersecurity Capability Maturity Model (C2M2). Version 1.1 February 2014. Department of Energy (DOE) and Department of Homeland Security (DHS). Disponível em: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-0. Acesso em: 22 de setembro de 2020.

United States of America (USA). 2020. Dictionary of Military and Associated Terms. Department of Defense – Government of United States of America.

Vedder, A. et al., eds. 2019. *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*. Intersentia, Cambridge, United Kingdom.

Zaballos, A. G. & Jeun, I. 2016. Best Practices for Critical Information Infrastructure Protection (CIIP) – Experiences from Latin America and the Caribbean and Selected Countries. Inter-American Development Bank (IDB) and the Korea Internet & Security Agency (KISA). Washington, D.C. 20577.

World Health Organization (WHO). 2014. Global Status Report Violence Prevention. United Nations – Geneva, Switzerland.