UFSM

InterAção

ISSN 2357-7975
ACESSO ABERTO

IA., Santa Maria, v. 17, n. 3, e98413, p. 1-32, 2026 • https://dx.doi.org/10.5902/2357797598413
Submissão: 25/08/2026 • Aprovação: 14/09/2026 • Publicação: 02/10/2026

Artigos Dossiê

O Sul Global e o dilema da segurança: ameaça doméstica e vigilância cibernética

The Global South and the security dilemma: domestic threat and cyber surveillance

Luiz Gustavo Lavandoski da Silva[I]
Eduardo Arthur Izycki[II]

[I]Universidade Federal do ABC, Santo André, SP, Brasil.
[II]Universidade de Brasília, Brasília, DF, Brasil

Resumo

Este trabalho analisa em que condições os Estados parte do Sul Global direcionam suas capacidades cibernéticas para o controle doméstico em vez da projeção externa de poder. Assim, o ponto de partida é a divergência entre o que a literatura de poder cibernético espera de uma potência e o emprego efetivamente observado na região, marcado pela vigilância de opositores políticos e da imprensa e pela interrupção de serviços de internet em momentos de instabilidade política. A justificativa proposta articula tanto a teoria da securitização, quanto a teoria dos complexos regionais de segurança para explicar esse tema através da sociologia histórica da formação do Estado, sustentando que, na ausência de um rival estatal recíproco capaz de securitizar o inimigo externo, e onde o aparato coercitivo foi historicamente construído para o controle interno, a capacidade cibernética é dirigida ao plano doméstico. Por meio de análise qualitativa comparada, examinaram-se três casos de ameaça predominantemente doméstica (Brasil, México e Etiópia) e o caso Índia-Paquistão, tomado como contraste por reunir uma rivalidade interestatal recíproca. Os resultados indicam que, sem um rival estatal externo, o uso documentado da capacidade cibernética tem sido doméstico, enquanto que Índia-Paquistão ativou também um vetor externo, sem abandonar o interno. Por fim, este artigo contesta a tese do déficit cibernético do Sul Global e reorienta o debate da magnitude das capacidades para a finalidade do seu emprego e para os mecanismos de controle necessários.

Palavras-chave: Poder cibernético; Sul Global; Vigilância cibernética; Formação do Estado

Artigo publicado por InterAção sob uma licença CC BY-NC-SA 4.0.

Abstract

This article examines the conditions under which Global South states direct their cyber capabilities toward domestic control rather than the external projection of power. The starting point is the divergence between what the cyber power literature expects of a cyber power and the use actually observed in the region, marked by the surveillance of political opponents and of the press and by the disruption of internet services in moments of political instability. The proposed framework draws on both securitization theory and regional security complex theory, explaining the phenomenon through the historical sociology of state formation and holding that, in the absence of a reciprocal state rival able to securitize an external enemy, and where the coercive apparatus was historically built for internal control, cyber capability is directed toward the domestic sphere. Through a qualitative comparative analysis, three cases of predominantly domestic threat (Brazil, Mexico, and Ethiopia) and the India-Pakistan case, taken as a contrast for combining a reciprocal interstate rivalry, were examined. The results indicate that, without an external state rival, the documented use of cyber capability has been domestic, while India and Pakistan also activated an external vector, without abandoning the internal one. Finally, the article challenges the thesis of a Global South cyber deficit and reorients the debate from the magnitude of capabilities toward the purpose of their use and the control mechanisms required.

Keywords: Cyber power; Global South; Cyber surveillance; State formation

1 INTRODUÇÃO

A visão tradicional do quinto domínio, potencializada pelos efeitos da globalização, da Revolução Industrial e do atual nível de evolução tecnológica, é defendida por pesquisadores que concebem o poder cibernético como um conjunto de diferentes capacidades viabilizadas pela dimensão cibernética (Nunes; Assunção; Brustolin, 2022). No âmbito das relações entre Estados, sobretudo nestes últimos anos, voltou a ser foco da discussão, a oportunidade de exploração da inovação tecnológica na competição militar, impulsionada pela literatura da revolução em assuntos militares, que analisa como as inovações tecnológicas afetam o equilíbrio de poder (Krepinevich, 1994) e desenvolvimento interno de um Estado, e que hoje encontra na corrida da Inteligência Artificial e na criptografia quântica a sua versão mais recente.

Nesse sentido, Malagutti e Gama Neto (2020) observam que a logística (*supply chain*) da dimensão cibernética cria pontos de estrangulamento pelo controle de tecnologias. Porém, existem oportunidades de projeção de *soft power* debatidas na literatura de Relações Internacionais (Nye, 2011), no mesmo sentido das versões de *software power*, que designam a capacidade político-estratégica de intervir na política externa de outro Estado por meio de software (Vilar-Lopes, 2016).

No contexto dos debates sobre o Sul Global, Devanny, Goldoni e Medeiros (2022) sustentam que o poder cibernético ocupa uma posição complexa e institucionalmente fragmentada nos debates brasileiros de segurança e defesa, marcada pela concepção estreita e militarizada do conceito e pela tensão entre a liderança do Gabinete de Segurança Institucional em segurança cibernética e a atribuição da defesa cibernética ao Ministério da Defesa. Nisso é possível identificar a configuração de uma dualidade, onde uma parte significativa de pesquisadores sustentam a existência de um déficit de poder cibernético na região, caracterizado tanto pela ausência de operações ofensivas de elevada complexidade quanto pela dependência estrutural de tecnologias desenvolvidas e fornecidas por atores do Norte Global (Calderaro; Craig, 2020). De outro lado, o conjunto de evidências produzido ao longo da última década mostra que muitos desses Estados desenvolveram e adquiriram capacidades cibernéticas de considerável sofisticação (Deibert, 2020; Feldstein, 2021).

O que tende a escapar às interpretações predominantes é a forma como essas capacidades são utilizadas, em vez de serem voltadas para a competição interestatal ou para a projeção de poder no Sistema Internacional (SI), como ocorre na contraparte setentrional, elas são predominantemente empregadas no plano doméstico, servindo a práticas de vigilância de opositores, monitoramento da imprensa e interrupção de serviços de internet em momentos de contestação ou instabilidade política. As revelações do *Pegasus Project*, que documentaram o uso de *spyware* contra jornalistas e defensores de direitos humanos em dezenas de países, e o registro de um número recorde de apagões de internet em 2024 ilustram a escala desse padrão na última meia década (Forbidden Stories, 2021; Access Now, 2025).

Essa diferença entre o que a literatura espera de uma potência cibernética e o que efetivamente se observa no Sul Global constitui o problema de pesquisa deste artigo. Assim, este trabalho busca apreciar **em que condições os Estados do Sul Global direcionam suas capacidades cibernéticas para o controle doméstico, em vez da projeção externa de poder?**

O argumento central deste artigo é sustentado pela premissa de casos onde não há um rival estatal recíproco capaz de sustentar a securitização do inimigo externo, e onde o aparato coercitivo foi historicamente construído para o controle interno, a capacidade cibernética é dirigida ao plano doméstico. Onde existe uma rivalidade interestatal recíproca e duradoura, ativa-se também um vetor externo, sem que o vetor doméstico desapareça.

Assim, através da abordagem qualitativa, utilizando a análise comparada, este trabalho buscou três casos típicos de ameaça predominantemente doméstica, sendo escolhidos pelos critérios de países do Sul Global o Brasil, o México e a Etiópia. Para além destes, escolhemos o caso da Índia–Paquistão, apresentado como contraste, ao demonstrar que, onde existe um rival externo recíproco capaz de sustentar a securitização do inimigo, o vetor externo atrai recursos de capacidade cibernética ofensiva. Esse contraste entre a rivalidade regional e o foco doméstico mostra que o desenvolvimento e o emprego de capacidades cibernéticas de caráter ofensivo estão orientados pelo processo discursivo de construção de ameaças, conforme desenvolvido na seção seguinte.

Este artigo não sustenta que os Estados do Sul Global devam abster-se de desenvolver suas capacidades ofensivas (complexo de desenvolvimento armamentista), mas que para Estados com limitações estruturais no acesso à tecnologia armamentista convencional (mísseis, sistemas de defesa e afins), o domínio cibernético oferece uma via assimétrica de dissuasão, de custo comparativamente baixo e de elevado potencial compensatório (Nye, 2017). O que o artigo identifica é influência da arquitetura institucional ao orientar o emprego de capacidades cibernéticas ofensivas, e, por essa razão, o Sul Global necessita de um debate de segurança próprio - que não se limite à defesa cibernética - em vez de importar molduras normativas estabelecidas a partir da realidade dos problemas do Norte Global (Lobato, 2024), conforme identificado nos Estudos de Segurança Internacional (ESI) por Buzan e Hansen (2012).

O artigo está organizado em seis seções, incluindo esta introdução. A segunda seção desenvolve o quadro teórico, articulando a teoria da securitização, a teoria dos complexos regionais de segurança e a literatura de poder cibernético, incluindo a distinção entre segurança e defesa cibernéticas e a gramática do "uso responsável".

A terceira seção completa o quadro com a sociologia histórica da formação do Estado e enuncia o mecanismo causal que sustenta o argumento. A quarta parte apresenta o desenho metodológico com a seleção dos casos, a operacionalização das variáveis e a análise dos casos. A quinta procede à comparação sistemática entre os casos. A sexta discute as implicações para o debate de ciberdefesa no Sul Global e as conclusões do trabalho.

2 A SECURITIZAÇÃO E A CONSTRUÇÃO SOCIAL DO CONCEITO DE AMEAÇA

Esta seção apresenta a construção social e conceitual do que se compreende por ameaça, partindo da gramática política pela qual as ameaças são construídas e legitimadas, a teoria da securitização, passando pelo conceito de complexo regional de segurança e chegando ao espaço cibernético como domínio emergente de disputas de poder no Sul Global. As condições histórico-estruturais que moldaram as capacidades coercitivas dos Estados, primeiro pilar do argumento, desenvolvidas na seção seguinte; esta seção trata do mecanismo discursivo que conecta essas condições à direção contemporânea do uso da capacidade cibernética.

Desenvolvida por Barry Buzan, Ole Wæver e Jaap de Wilde (1998) no âmbito da Escola de Copenhague, a teoria da securitização constitui o pilar analítico deste artigo. Formulada no contexto do pós-Guerra Fria, quando os estudos de segurança internacional passavam por uma profunda transformação, marcada pela transição de pólos de poder, pela inclusão de novas perspectivas estratégicas na agenda e pelo surgimento de atores não estatais com capacidade de influência no SI, a teoria rompeu com a concepção objetivista da ameaça e propôs uma abordagem construtivista e discursiva.

O ponto central da teoria é que a segurança não é um estado de fato, mas um ato de fala (*speech act*), pelo qual um ator "securitizante" (geralmente, mas não exclusivamente, o Estado) declara que determinado fenômeno representa uma ameaça existencial a um objeto referente (o Estado, uma nação, o meio ambiente, indivíduos, o ciberespaço) e, com isso, reivindica o direito de adotar medidas de exceção que extrapolam os limites ordinários da política (Buzan; Wæver; De Wilde, 1998, p. 26-27). A securitização não pressupõe a existência objetiva de uma ameaça, na verdade, o que torna uma questão um problema de segurança é o processo político pelo qual ela é enquadrada como tal, e esse processo só se completa com a aceitação da "audiência" relevante.

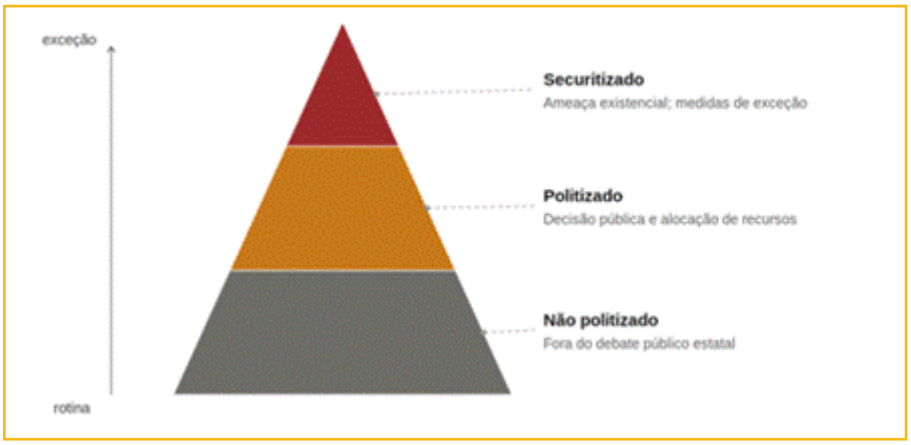
Nos termos dos autores, "a securitização bem-sucedida não é decidida pelo securitizador, mas pela audiência do ato de fala de segurança" (Buzan; Wæver; De Wilde, 1998, p. 31). Essa dimensão relativa à audiência é relevante, já que, em contextos autoritários ou semiautoritários, a "audiência" pode ser coercitivamente constituída, o que reduz o limiar para securitizações bem-sucedidas de ameaças domésticas.

Outro elemento central da teoria é a ideia da politização, que é uma "continuação" da ideia anterior que vai do não politizado ao securitizado, conforme apresentamos na Figura 1 a seguir. Compreende-se que a posição de uma questão neste espectro não é determinada por sua natureza objetiva e pode variar substancialmente entre Estados e ao longo do tempo. Logo, alguns securitizam a religião, outros a cultura, outros os movimentos sociais, variando conforme os seus objetivos políticos (Buzan; Wæver; De Wilde, 1998, p. 23-24).

Os autores também apontam uma dimensão crítica, sobre a qual os próprios fazem um alerta:

> a segurança nacional não deve ser idealizada. Ela funciona para silenciar a oposição e tem dado aos detentores do poder muitas oportunidades de explorar 'ameaças' para propósitos domésticos, para reivindicar o direito de lidar com algo com menos controle e constrangimento democrático. (BUZAN; WÆVER; DE WILDE, 1998, p. 29, traduzido pelos autores).

Figura 1 – Espectro de politização da Escola de Copenhague



Fonte: Autores (2026)

Essa dimensão instrumental da securitização, sua função como veículo de legitimação do poder, é central para compreender por que governos do Sul Global securitizam ameaças domésticas e mobilizam capacidades cibernéticas para o controle interno, mesmo quando os documentos oficiais e estratégias nacionais invocam ameaças externas.

A teoria expande, ainda, o conceito de segurança para além do setor militar-político convencional, reconhecendo cinco setores (militar, político, econômico, societal e ambiental), cada um com os seus próprios objetos referentes e lógicas de ameaça existencial. No setor político, o mais diretamente ligado ao presente trabalho, as ameaças existenciais são definidas em termos da soberania e da autoridade governante. Logo, "a soberania pode ser existencialmente ameaçada por qualquer coisa que questione o reconhecimento, a legitimidade ou a autoridade de governo" (Buzan; Wæver; De Wilde, 1998, p. 22-23). Isso mostra que oposições políticas, movimentos separatistas ou insurgências internas são, do ponto de vista do ator securitizante, ameaças existenciais ao mesmo título que uma invasão militar estrangeira, o que justifica, na lógica do regime, o recurso a instrumentos extraordinários, incluindo a vigilância massiva.

2.1. Complexos regionais de segurança e a geografia da ameaça

A securitização mostra como uma ameaça é construída através do discurso, mas não explica a razão de certas ameaças se tornarem prioritárias para as elites. A teoria dos complexos regionais de segurança, formulada por Buzan e Wæver (2003), ajuda a preencher essa lacuna. Para os autores, a interdependência de segurança não se espalha de maneira uniforme pelo sistema internacional, mas se concentra em aglomerados regionais, nos quais as preocupações de segurança dos Estados estão tão entrelaçadas que não faz sentido analisá-las de forma isolada.

Dessa formulação decorre uma consequência metodológica que orienta todo este artigo: as dinâmicas de ameaça identificadas no Norte Global não se transpõem automaticamente para o Sul Global, porque cada complexo regional produz o seu próprio pacote de ameaças, amizades e rivalidades. Essa é a razão pela qual o debate de segurança e defesa cibernéticas do Sul Global e suas diferentes regiões precisa ser conduzido de forma independente, a partir das dinâmicas regionais que efetivamente o constituem.

O que interessa diretamente ao argumento deste trabalho é a posição que cada Estado ocupa dentro do seu complexo regional. Essa posição determina se ele convive ou não com um adversário estatal recíproco, capaz de securitizar de forma sustentada o ambiente externo. Em regiões marcadas por uma rivalidade interestatal duradoura, como ocorre entre Índia e Paquistão, a securitização do inimigo externo se apoia em uma base material concreta, o que a torna recorrente e crível para a audiência interna. Já em regiões relativamente amistosas ou sem rivais simétricos, caso de boa parte da América do Sul e da África subsaariana, a ameaça externa perde força no discurso, e a securitização se volta para dentro do próprio Estado.

O complexo regional situa a ameaça no espaço e permite antecipar, a partir da configuração de cada região, qual objeto referente costuma ser securitizado. Essa antecipação orienta, nas seções empíricas, a expectativa sobre a direção que as capacidades cibernéticas tendem a assumir em cada caso.

2.2. Segurança, defesa cibernéticas e a gramática do "uso responsável"

A securitização explica como o conceito de ameaça é construído e o complexo regional indica como ela se orienta em determinados contextos regionais. No debate brasileiro, a securitização do ciberespaço já foi tratada como processo discursivo que enquadra o domínio cibernético como questão de segurança nacional (Medeiros; Goldoni, 2019).

Esta, por sua vez, designa o conjunto de práticas de proteção de sistemas, redes e dados contra ameaças de natureza variada (crime cibernético, fraude, incidentes acidentais, ataques a serviços, inteligência), que é atribuído tipicamente a autoridades civis, policiais e reguladoras, com foco na resiliência da sociedade e proteção tecnológica (Canongia; Mandarino Junior, 2010). A literatura brasileira de defesa cibernética tem sistematizado essa fronteira e as suas implicações institucionais (Vilar-Lopes, 2016; Brustolin, 2019; Nunes; Assunção; Brustolin, 2022).

A defesa cibernética, por sua vez, constitui um subconjunto de natureza estatal-militar, onde se orienta à proteção de infraestruturas críticas e de ativos de defesa contra ameaças de origem estatal ou equiparada, e compreende a condução de operações no espaço cibernético, incluindo capacidades ofensivas e de dissuasão (Brustolin, 2019).

Nas potências cibernéticas do Norte Global, essa fronteira é institucionalmente demarcada, nos Estados Unidos por exemplo, a proteção civil de redes cabe a uma agência própria, enquanto as operações militares se concentram em um comando combatente dedicado; já no Reino Unido, a proteção civil (*National Cyber Security Centre*) e as operações militares (*National Cyber Force*) cabe igualmente a órgãos distintos.

Essa demarcação clara para Defesa Cibernética pressupõe um ambiente de rivalidade interestatal que assinala um alvo externo claro, pressuposto que não se verifica na maior parte do Sul Global, onde a fronteira entre defesa cibernética, inteligência e segurança pública tende a ser porosa.

Foi nas potências do Norte Global que a moldura normativa do uso da capacidade cibernética foi formulada. Os Estados Unidos assumiram publicamente uma postura ofensiva com as doutrinas *defend forward* e *persistent engagement* (US Department of Defense, 2018); o Reino Unido revelou o funcionamento da sua National Cyber Force e codificou o conceito de "poder cibernético responsável", enunciando princípios de operação (responsabilidade, precisão e conformidade legal e ética) que buscam legitimar o emprego ofensivo (National Cyber Force, 2023); e os Países Baixos institucionalizaram um Defence Cyber Command com capacidade ofensiva assumida. Em todos os casos, a legitimação da capacidade repousa sobre uma realidade estratégica de competição interestatal.

Essa gramática migrou para o plano multilateral sob o rótulo de "comportamento responsável de Estados no ciberespaço". O relatório do Grupo de Peritos Governamentais das Nações Unidas (UNGGE) de 2015 estabeleceu onze normas voluntárias e não vinculantes, entre elas a proteção de infraestrutura crítica, a integridade da cadeia de suprimentos e o respeito aos direitos humanos, posteriormente endossadas pela Assembleia Geral (United Nations, 2015).

A estrutura foi consolidada em 2021, quando o Grupo de Trabalho de Composição Aberta (OEWG) reuniu o conjunto dos Estados-membros em torno de um quadro comum de comportamento responsável (United Nations, 2021). O traço desse regime que importa ao argumento é a orientação interestatal, como os limites para o que um Estado pode fazer contra outro Estado, presumindo um ambiente de rivalidade externa.

Apenas recentemente a governança internacional voltou-se para a face da capacidade cibernética que mais afeta o Sul Global: a proliferação de ferramentas comerciais de intrusão. O Processo de Pall Mall, lançado por Reino Unido e França em 2024, foi a primeira iniciativa multilateral dedicada a conter a proliferação e o "uso irresponsável" de *commercial cyber intrusion capabilities*, categoria que abrange o spyware mercantil do tipo empregado nos casos aqui examinados (Pall Mall Process, 2024).

A iniciativa avançou com a adoção de um Código de Conduta para Estados em 2025 (Pall Mall Process, 2025). Trata-se, porém, de um regime nascente, liderado por atores do Norte e centrado sobretudo na regulação da oferta (os fornecedores), o que deixa em aberto a disciplina da demanda, isto é, dos Estados que dirigem essas ferramentas contra as suas próprias sociedades.

O critério do "uso responsável" foi regulado para a realidade estratégica de potências que enfrentam adversários externos recíprocos, na maioria dos Estados do Sul Global, porém, essa dimensão interestatal é estrategicamente vazia. O regime normativo dominante regula, assim, uma ameaça que ali pouco se manifesta e permanece em boa medida silente sobre a que de fato se manifesta, já que o emprego doméstico da capacidade cibernética contra a oposição, a imprensa e a dissidência. Em consonância com a lição dos complexos regionais de segurança (Buzan; Wæver, 2003), transpor esse quadro sem mediação é universalizar uma experiência particular do Norte.

3 FORMAÇÃO DO ESTADO E CAPACIDADES MILITARES: POR QUE OS ESTADOS CONSTROEM O QUE CONSTROEM

Estados com recursos parecidos constroem aparatos coercitivos diferentes, enquanto alguns os orientam para a competição externa, outros os voltam para o controle da própria população. Fatores históricos e institucionais influenciam essa decisão. O tipo de ameaça que um Estado precisou enfrentar para sobreviver moldou o tipo de capacidade que ele desenvolveu, e essa orientação inicial costuma se reproduzir quando novas tecnologias coercitivas, como as cibernéticas, se tornam disponíveis. Compreender a direção do uso da capacidade cibernética no Sul Global exige recuar até a formação do Estado e ao problema clássico de por que os governantes constroem o que constroem.

A escolha desse recorte teórico responde a uma lacuna do debate. Construída a partir da experiência das grandes potências, para as quais a competição interestatal é

o horizonte natural do domínio cibernético, a literatura sobre poder cibernético tende a esperar dos Estados da região um comportamento que a sua trajetória histórica não sustenta. A sociologia histórica do Estado oferece a correção, porque explica por que a maioria desses Estados desenvolveu instituições coercitivas voltadas para dentro e por que essa orientação persiste quando eles adquirem novas capacidades.

3.1 A tese bélica e o padrão europeu

O ponto de partida é a tese bélica da formação do Estado, associada sobretudo a Tilly (1990). Na Europa moderna, a guerra interestatal recorrente obrigou os governantes a extrair recursos da população em escala crescente, e essa extração exigiu burocracia fiscal e um aparato militar permanente. A competição entre unidades políticas funcionou como um filtro, no qual sobreviveram as que conseguiram converter capital e coerção em capacidade organizada de fazer a guerra. O Estado nacional moderno emergiu como subproduto desse processo, dotado de instituições capazes de penetrar o território e mobilizar a sociedade para o conflito. A máxima tillyiana, a ideia de que o Estado faz a guerra e a guerra faz o Estado, descreve mais do que história, podendo ser equiparada a um fenômeno causal.

Tilly (1985) descreveu a construção do Estado como uma atividade análoga ao crime organizado, na qual o governante oferece proteção contra ameaças que ele próprio ajuda a produzir e cobra por isso na forma de impostos e obediência. Essa imagem ilumina a natureza coercitiva do Estado antes de qualquer verniz de legitimidade e dialoga com a definição weberiana do Estado como a organização que reivindica com êxito o monopólio do uso legítimo da força em um território (Weber, 2011). O monopólio da violência consolidou-se ao cabo de séculos de competição armada, como resultado incerto desse processo.

A sociologia histórica desenvolveu esse núcleo em várias direções. Hintze (1975), por exemplo, argumentou que a forma do Estado depende da pressão do sistema internacional e da organização militar que ela exige, e Mann (1986) situou o

desenvolvimento do poder estatal na articulação entre diferentes redes de poder social. Downing (1992) e Ertman (1997) mostraram como diferenças na mobilização militar ajudam a explicar trajetórias europeias rumo ao constitucionalismo ou ao absolutismo, enquanto Porter (1994) e Spruyt (1994) situaram na guerra e na mobilização de recursos para o conflito o fundamento do Estado moderno e a prevalência do próprio formato estatal soberano.

Esse programa de pesquisa consolidou-se na agenda que devolveu o Estado ao centro da análise social (Evans; Rueschemeyer; Skocpol, 1985). Skocpol (1979) havia demonstrado, no estudo das revoluções, que o Estado deve ser tratado como uma organização com interesses e capacidades próprias, com autonomia relativa diante das forças sociais que o cercam. Essa autonomia importa para o argumento, porque significa que o aparato de segurança tem uma trajetória institucional que condiciona o seu comportamento futuro. As capacidades construídas em um período moldam as opções disponíveis no período seguinte, e a orientação inicial do aparato tende a se perpetuar.

Se a guerra externa recorrente centralizou e disciplinou o Estado europeu, então a ausência dessa pressão deveria produzir Estados com outra trajetória e outra orientação coercitiva. É exatamente o que se observa fora do núcleo europeu, onde a variável que moveu a formação do Estado assumiu valores distintos.

3.2 As duas faces do poder estatal e a virada cibernética

Para ligar a formação do Estado à direção do uso da força, é útil a distinção de Mann (1984) entre poder despótico e poder infraestrutural. O poder despótico mede a margem de ação da elite estatal sobre a sociedade sem negociação. O poder infraestrutural mede a capacidade de o Estado penetrar o território e pôr suas decisões em prática ao longo da jurisdição. As duas dimensões variam de forma independente, e um Estado pode ter grande margem arbitrária e ainda assim controlar mal a periferia.

Uma das dimensões do poder infraestrutural é a capacidade de tornar a sociedade legível, de registrar e classificar populações e territórios (Soifer; Com Hau, 2008). Scott

(1998) mostrou como os projetos modernos de governo dependem de instrumentos de legibilidade que permitiram ao Estado enxergar o que pretendia administrar. A vigilância, nessa chave, é uma tecnologia de poder infraestrutural, porque amplia a visão do Estado sobre a sociedade. Giddens (1985) levou o ponto adiante ao definir o Estado moderno como um contêiner de poder que se apoia na vigilância, entendida como coleta e controle de informação sobre a população. Quando um Estado adquire capacidade de interceptação e monitoramento, ele expande uma função que já é central no seu poder infraestrutural.

Muitos Estados fora do núcleo europeu combinam ambição despótica com poder infraestrutural reduzido, porque controlam mal a periferia e enxergam de forma precária o que acontece dentro das próprias fronteiras. Para eles, a capacidade cibernética ofensiva funciona como um atalho, porque promete o alcance sobre a população que a construção histórica do aparato não produziu. A demanda por capacidade cibernética voltada para dentro nasce, em boa parte, dessa lacuna.

A orientação interna do aparelho tem lógica própria. Greitens (2016) mostra que os governantes vivem um dilema entre se proteger da mobilização popular e se proteger de golpes das próprias elites, e que essa escolha define o desenho das instituições de segurança. Aparatos construídos para vigiar e conter a população desenvolvem inteligência interna e redes de informantes, e já operavam com fichários e escutas antes do spyware. Quando as tecnologias cibernéticas chegam a esse ambiente, são absorvidas por instituições cuja missão histórica é o controle interno e assumem a direção que essa missão impõe.

A tecnologia da informação muda a escala do problema sem mudar a sua natureza. Xu (2021) desenvolve uma teoria informacional da repressão e mostra que a vigilância resolve o problema clássico do governante, que é não conhecer as preferências reais dos cidadãos. Ao identificar opositores com precisão, ela permite trocar a repressão indiscriminada por uma repressão seletiva, que custa menos em termos políticos. Gohdes (2020) mostra que o controle do acesso à internet virou

instrumento de violência estatal, e Feldstein (2021) e Deibert (2020) documentam a difusão global dessas tecnologias e o mercado comercial de vigilância que a sustenta.

A natureza dual da capacidade cibernética reforça o efeito, já que a mesma capacidade usada contra um adversário externo serve para monitorar a oposição interna. Isso permite apresentar o investimento em vigilância sob o rótulo neutro da defesa cibernética e reduz o custo político da compra. Soma-se a isso a difícil atribuição do uso das ferramentas cibernéticas, o que torna uma ferramenta menos visível que a repressão física. O mercado comercial de intrusão vende capacidade pronta para uso, sem que o comprador precise dominar a complexidade técnica por trás dela. Logo, para um Estado de poder infraestrutural historicamente baixo, essa oferta resolve um problema antigo de alcance a um custo modesto, e o faz com fornecedores estrangeiros que retêm o domínio da tecnologia (Calderaro; Craig, 2020; Malagutti; Gama Neto, 2020).

A construção da ameaça depende de uma audiência disposta a aceitar o movimento securitizador (Buzan; Wæver; De Wilde, 1998), e a orientação histórica do Estado condiciona quais ameaças soam plausíveis para essa audiência. Onde o aparato foi construído para o controle interno e não há rival externo crível, a securitização convincente costuma ser a do inimigo doméstico, e é para ele que a capacidade se dirige. A herança institucional e o discurso de segurança operam na mesma direção e reforçam um ao outro.

4 ANÁLISE DOS CASOS

Os casos selecionados são examinados quanto à natureza dominante da ameaça securitizada, considerando a sua posição no complexo regional de segurança, e, também, para onde se dirige o emprego das suas capacidades cibernéticas.

A variável independente é a presença de um adversário estatal recíproco, entendida como a existência de uma rivalidade interestatal material e sustentada no complexo regional. A variável dependente é a direção observada do uso da capacidade

cibernética, classificada como interna, externa ou mista, com base em evidências documentadas na última década.

Os dados utilizados nos estudos de caso provêm de relatórios públicos produzidos por empresas de segurança cibernética e consórcios jornalísticos internacionais, complementados por documentos oficiais, triangulados para validação, na medida do possível. Cabe destacar que a natureza clandestina das operações cibernéticas impõe um viés de visibilidade, já que apenas as campanhas detectadas entram no registro público, logo, campanhas bem sucedidas provavelmente existem e ainda não são de conhecimento público. A comparação qualitativa de poucos casos, por sua vez, permite avaliar a plausibilidade do mecanismo proposto (George; Bennett, 2005), sem pretensão de generalização estatística.

A referência são os Estados do Sul Global que adquiriram ou desenvolveram capacidade cibernética ofensiva (Izycki, 2022), o que exclui, por definição, um grande volume de países que não demonstraram capacidade ofensiva. Contudo, não há pretensão estatística para extrapolar o estudo além desses casos, apenas demonstrar a relação causal entre a ausência de rivalidade regional e o foco doméstico de capacidades cibernéticas.

Os três casos de foco predominantemente doméstico (Brasil, México e Etiópia) se baseiam em complexos regionais distintos e com trajetórias de formação estatal diversas que securitizam objetos referentes distintos. Porém, o padrão que exibem é consistente com evidências transnacionais como os bloqueios de internet e a proliferação de spyware comercial (Access Now, 2025; Feldstein, 2021).

A seleção dos três casos de ameaça doméstica não se limitou ao critério de ausência de rival estatal recíproco; buscou-se maximizar a variação de outros fatores potencialmente concorrentes - complexo regional de segurança, regime político e objeto referente securitizado. Brasil e México são democracias eleitorais inseridas em complexos regionais distintos (América do Sul de baixa conflitualidade; América do Norte/Central sob assimetria com os EUA), enquanto a Etiópia opera sob um regime

de federalismo étnico historicamente menos democrático; os três, ainda, securitizam objetos referentes diferentes (crime organizado, narcotráfico, dissidência étnica). Essa diversidade deliberada reduz a plausibilidade de explicações alternativas ancoradas em região, regime ou tipo específico de ameaça.

Outros Estados do Sul Global com capacidade ofensiva documentada por Izycki (2022), como Vietnã, Marrocos e Nigéria, foram excluídos por dois motivos. O Vietnã mantém disputa territorial ativa e recorrente com a China no Mar do Sul da China, não preenchendo o critério de ausência de rival estatal recíproco que define o universo de casos deste grupo. A Nigéria e o Marrocos, por sua vez, carecem até o momento de investigação forense pública e triangulável equivalente à que sustenta os três casos aqui selecionados, o que reduz o padrão de evidência disponível.

As subseções seguintes percorrem os casos na ordem em que variam quanto ao adversário externo recíproco: em cada um, o exame situa primeiro a posição regional e a ameaça securitizada dominante e observa, em seguida, direção documentada do uso das capacidades cibernéticas no período recente.

4.1. México

O México não convive com um rival estatal recíproco. Sua relação externa mais relevante é assimétrica, com os Estados Unidos, um parceiro que não pode ser securitizado de forma sustentada como inimigo militar externo; mesmo diante das inflexões recentes da política externa estadunidense, a relação é assimétrica demais para isso. A ausência de adversário externo simétrico desloca a securitização para o plano interno, onde o objeto referente é a ordem pública ameaçada pelo crime organizado.

Desde a "declaração da guerra" ao narcotráfico, em 2006, o combate aos cartéis tornou-se o ato de fala dominante da segurança mexicana e a justificativa central para a expansão das capacidades de vigilância. A própria Estratégia Nacional de Cibersegurança organiza o domínio em torno do cibercrime e da segurança pública, sem eleger um adversário estatal externo como objeto referente (México, 2017).

A trajetória do aparato de segurança mexicano ajuda a entender essa direção. Ao longo do século XX, sob a hegemonia do Partido Revolucionário Institucional, o Estado desenvolveu instrumentos de controle político e de monitoramento da oposição muito antes de qualquer ameaça externa relevante. A militarização da segurança pública a partir de 2006 reforçou um aparato já orientado para dentro, agora encarregado de enfrentar os cartéis com meios de guerra. A capacidade cibernética foi enxertada nessa estrutura e herdou a sua vocação doméstica.

O caso mais documentado é o do programa Pegasus, da israelense NSO Group. O México é um dos maiores clientes da empresa e a investigação do Pegasus Project, em 2021, indicou que o maior número de alvos, cerca de quinze mil (Forbidden Stories, 2021). As vítimas confirmadas por análise forense incluem a jornalista Carmen Aristegui e advogados ligados ao caso Ayotzinapa, entre outros ativistas e opositores. A escolha dos alvos revela a lógica do uso. O programa foi de fato empregado contra figuras do crime organizado, como no caso da captura de Joaquín Guzmán, mas o conjunto documentado de alvos excede sistematicamente esse mandato e recai sobre quem fiscaliza o poder, alcançando jornalistas, advogados e opositores.

O padrão mostrou-se resistente à alternância política: mesmo após a promessa do governo de Andrés Manuel López Obrador de interromper a vigilância, relatórios posteriores documentaram a continuidade do emprego do Pegasus pelas Forças Armadas contra defensores de direitos humanos (R3D, 2022), o que reforça a leitura de que a ferramenta serve sobretudo à proteção do aparato de poder.

As primeiras revelações sobre o uso do Pegasus no México, em 2017, já apontavam um ecossistema de vigilância alimentado por múltiplas agências federais e estaduais, com contratos que ultrapassavam o objetivo declarado de combate ao crime.

Não há, em contrapartida, registro de operação cibernética ofensiva mexicana contra outro Estado: a ameaça do narcotráfico é concreta e violenta, porém o emprego documentado da capacidade excede o seu enfrentamento e alcança a imprensa e a oposição.

4.2. Etiópia

A Etiópia possui tensões regionais, com o Egito, em torno da Grande Barragem do Renascimento, e com a Eritreia, mas nenhum deles se traduziu em uma díade cibernética ativa. O eixo estruturante da política de segurança etíope é doméstico e organiza-se em torno do federalismo étnico, principalmente com as tensões entre a Frente de Libertação do Povo do Tigré (TPLF) e a mobilização das comunidades Oromo. É esse o conjunto de ameaças que o Estado securitiza, e foi para ele que a capacidade cibernética foi dirigida.

A formação do Estado reforça historicamente o argumento por outro caminho. A Etiópia escapou à colonização direta, mas construiu um aparato coercitivo voltado à integração forçada de um território plural e à contenção de movimentos centrífugos em suas diferentes regiões. O arranjo de federalismo étnico adotado em 1995 institucionalizou a gestão multiétnica como tarefa central do Estado, e foi essa tarefa que orientou o desenvolvimento das suas capacidades de segurança. Na percepção dos governantes, o inimigo relevante sempre esteve dentro das fronteiras ou entre os exilados que contestam o regime a partir de fora, o que direcionou o uso das capacidades cibernéticas ofensivas.

A Citizen Lab documentou o emprego do *FinSpy*, da Gamma Group, do RCS, da Hacking Team, e, mais tarde, do produto PSS, da israelense Cyberbit, em campanhas contra dissidentes da diáspora Oromo radicados na Europa e na América do Norte (Marczak et al., 2017). O alvo foi a oposição no exílio, alcançada fora das fronteiras, porém por motivação inteiramente doméstica, fenômeno que a literatura designa como repressão transnacional (Schenkkan; Linzer, 2021). A dissidência no exílio não constitui um alvo no sentido interestatal, pois é a mesma oposição doméstica securitizada perseguida para além das fronteiras. Logo, a motivação política orienta a capacidade ofensiva e não a a localização dos alvos.

Durante a guerra do Tigré, entre 2020 e 2022, o governo combinou bloqueios de internet, registrados de forma sistemática pelo monitoramento independente

de bloqueios, com operações de desinformação, transformando a conectividade digital em instrumento do conflito interno (Access Now, 2025). Nenhuma operação cibernética ofensiva etíope contra o Egito ou a Eritreia foi documentada, apesar das tensões regionais existentes. A capacidade foi mobilizada para a guerra civil e para a vigilância da dissidência, logo a projeção externa permaneceu ausente.

O caso etíope inscreve-se, ainda, em um padrão africano mais amplo de importação de vigilância, no qual fornecedores europeus, israelenses e chineses deram a governos do continente, um alcance sobre a dissidência que o seu poder infraestrutural histórico não proporcionou. A ausência de um adversário estatal recíproco consolidado, somada a uma agenda de segurança centrada na coesão territorial, manteve o uso voltado para o controle da oposição e para os conflitos internos.

4.3. Brasil

O Brasil está inserido em uma região de baixa conflitualidade interestatal, sem rival recíproco no continente meridional e com uma tradição diplomática de resolução pacífica de controvérsias e de não-intervenção. A securitização brasileira tem sido predominantemente doméstica, ligada à segurança pública, com uma camada adicional na proteção de infraestrutura crítica e de grandes eventos, como a Copa do Mundo de 2014 e os Jogos Olímpicos de 2016, que impulsionaram a institucionalização da defesa cibernética.

A herança institucional aponta na mesma direção. O aparato de inteligência atual descende de estruturas montadas durante o regime militar sob a doutrina do inimigo interno, quando o Serviço Nacional de Informações organizou a vigilância da sociedade em nome da segurança nacional (Stepan, 1988). A redemocratização reformou o sistema e criou a Agência Brasileira de Inteligência (ABIN), porém a orientação histórica para o monitoramento doméstico não desapareceu por completo, e ressurge nos episódios mais sensíveis do período recente. A forma como a atividade de inteligência aparece nos documentos de defesa recentes confirma a permanência dessa orientação (Martins, 2017).

O país construiu o Comando de Defesa Cibernética (ComDCiber) e organizou suas capacidades em torno da proteção de redes e da resposta a incidentes, com a defesa cibernética reconhecida como setor estratégico (Oliveira; Portela, 2017). A concepção que orienta esse arranjo entende o poder cibernético como instrumento operacional da esfera militar, voltado à proteção e à resposta a incidentes (Devanny; Goldoni; Medeiros, 2022). A Política Nacional de Defesa aprovada em 2024 reafirma o objetivo declarado de autonomia tecnológica (Brasil, 2024).

No plano do uso efetivo, porém, os episódios mais significativos são domésticos. Há registros de monitoramento em contextos de protesto (2013) e nas mobilizações de 2018, quando o aparato de segurança acompanhou manifestantes e organizações da sociedade civil. Porém, o caso mais notório envolveu servidores da ABIN que haviam utilizado a ferramenta *FirstMile*, da israelense Cognyte, para geolocalizar telefones celulares em tempo real sem autorização judicial. As investigações indicaram o monitoramento de até dez mil aparelhos por ano entre 2019 e 2021, com alvos que incluíam opositores e jornalistas, além de ministros do Supremo Tribunal Federal (CNN Brasil, 2023).

No Brasil há registro de fontes abertas sobre operação cibernética ofensiva contra o Paraguai, mas não houve confirmação por documentos ou investigação oficial. Em que pese exercícios de defesa como o Guardião Cibernético (em sua sétima edição), a projeção externa brasileira do poder cibernético permanece incipiente, sendo notórios apenas as ações ofensivas contra alvos domésticos, sem a devida supervisão legal.

4.4. O Caso Índia–Paquistão

A relação entre Índia e Paquistão, inseridos no complexo de segurança sul-asiático, o mais militarizado entre os casos, representa o contraste onde cada país constitui, para o outro, o adversário estatal recíproco ausente nos casos anteriores. À díade recíproca soma-se, do lado indiano, a tensão sustentada com a China na

fronteira do Himalaia, e, em ambos os países, uma agenda interna de securitização: o separatismo na Caxemira e a insurgência maoísta, na Índia; o Tehrik-i-Taliban Paquistanês e a militância no Baluchistão, no Paquistão. Observamos tanto o vetor externo quanto o doméstico.

Em termos de ações cibernéticas ofensivas, os dois países empregam suas capacidades mutuamente. A Índia é associada ao grupo SideWinder, ativo desde 2012 e atribuído a interesses indianos com confiança significativa por empresas de inteligência de ameaças, dedicado à espionagem contra governo e forças armadas do Paquistão e da China. A análise técnica identificou um conjunto de ferramentas dedicado, batizado de StealerBot, e registrou a ampliação recente dos alvos para a infraestrutura marítima e o setor nuclear sul-asiático, indício de um interesse de inteligência tipicamente interestatal (Kaspersky, 2025).

O Paquistão, por sua vez, é associado ao grupo Transparent Tribe, também conhecido como APT36[I], voltado à espionagem contra militares e órgãos de governo da Índia, com ferramentas adaptadas inclusive aos sistemas de base Linux adotados pelo setor público indiano, o que indica um esforço sustentado e orientado ao alvo estatal externo (Cisco Talos, 2022).

Os dois países demonstraram, portanto, um esforço de atuação cibernética dirigida a um Estado rival, algo que não esteve presente nos três primeiros casos do Sul Global, onde predominava a orientação doméstica que a Índia-Paquistão não exibia.

Por outro lado, a presença da ameaça externa não suprime as ações contra alvos domésticos. A Índia, por exemplo, figura entre os clientes do Pegasus, com alvos de oposição e jornalistas documentados em 2021 (Forbidden Stories, 2021), e lidera, entre as democracias, os bloqueios de internet como instrumento de contenção da ordem pública, registrou oitenta e quatro apagões em 2024 (Access Now, 2025). O Paquistão também mantém significativo controle da internet por meio da sua autoridade de telecomunicações, incluindo bloqueios de internet em períodos de protesto e nas regiões de militância do Baluchistão.

[I] Transparent Tribe, grupo de ameaça persistente avançada focado em ciberespionagem ligado ao Paquistão.

Os dois países apresentam postura mista (o doméstico e o interestatal), o que reforça a percepção de que Estados desenvolvem capacidade cibernética ofensiva quando possuem uma ameaça externa que torna a securitização do oponente sustentável perante a audiência interna. Além disso, a direção do uso responde à configuração do complexo regional de segurança do sul da Ásia.

5 ANÁLISE COMPARATIVA E IMPLICAÇÕES PARA A CIBERDEFESA NO SUL GLOBAL

5.1 O padrão observado e a direção do uso

O Quadro 1 demonstra que nos três casos sem adversário estatal recíproco, o uso documentado da capacidade cibernética foi doméstico, apesar das diferenças do complexo regional de segurança e de regime políticos entre os países. De outro vértice, no caso da Índia e do Paquistão, contexto com rivalidade recíproca externa, ambos os Estados desenvolveram vetores externos ofensivos, sem contudo, abandonar o uso doméstico.

Quadro 1 — Configuração regional e direção do uso da capacidade cibernética

Caso	Rival estatal recíproco? (VI)	Objeto securitizado	Evidência central	Uso da Capacidade Cibernética
México	Não. Relação assimétrica com os EUA	Narcotráfico	Pegasus (NSO Group): imprensa, ativistas e oposição	Doméstico
Brasil	Não. América do Sul com baixa conflitualidade interestatal	Crime Organizado	FirstMile (Cognyte): opositores, jornalistas e ministros do STF	Doméstico
Etiópia	Não. Conflito com a Eritreia, mas diferença de capacidades acentuada	Coesão territorial / dissidência (TPLF, Oromo)	Spywares comercial contra a diáspora	Doméstico (alvos domésticos no exterior)
Índia–Paquistão	Sim. Díade recíproca e duradoura (incluindo tensão Índia–China)	Inimigo externo + insurgência interna	SideWinder / APT36 em espionagem, além do Pegasus e bloqueios de internet no plano interno	Doméstico e interestatal

Fonte: Autores (2026)

O mecanismo proposto conecta a ausência de ameaça externa e a securitização perante a audiência interna ao uso da capacidade cibernética (Buzan; Wæver; De Wilde, 1998).

No México, a audiência doméstica aceitou a securitização do crime organizado, e foi sob esse enquadramento que a capacidade de vigilância se expandiu e transbordou para alvos políticos. No Brasil o crime organizado se afigura como ameaça interna de segurança e o uso político deriva deste ponto, mas o país não conta com rival regional compatível. De forma similar, o risco de separatismo multiétnico sedimenta o uso de capacidades cibernéticas contra alvos domésticos na Etiópia. Em contrapartida, no Sul da Ásia, as crises de fronteiras com a China e a tensão na Caxemira mantêm crível a securitização do inimigo externo e tornam racional o investimento contínuo em espionagem interestatal tanto por Índia quanto Paquistão. Assim, onde a ameaça externa não se sustenta, a securitização migra para objetos domésticos como a ordem pública e a estabilidade do regime, o que enviesa internamente o uso da capacidade cibernética.

A hipótese do regime autoritário como causa explicativa deve ser afastada, pois México, Brasil e Índia são democracias eleitorais e figuram entre os usuários documentados de uso de capacidade cibernética contra alvos domésticos. Outra hipótese rechaçada seria o nível de capacidade ofensiva, pois o México é um dos maiores compradores de spyware sem nunca converter esse recurso em projeção externa, enquanto Índia e Paquistão sustentam campanhas interestatais duradouras com recursos limitados cibernéticos próprios. Logo, o que permanece constante é o referente à ameaça externa securitizada.

O caso etíope reforça o argumento, pois ao perseguir dissidentes da diáspora Oromo na Europa e na América do Norte, a Etiópia projetou sua capacidade para fora das fronteiras movido, mas motivado por agenda doméstica com a oposição no exílio, prática que a literatura recente nomeia repressão transnacional (Schenkkan; Linzer, 2021).

O fenômeno mostra que a dicotomia entre uso interno e uso externo não é um critério fixo e exclusivo de países do Sul Global e Norte Global. Há contra-exemplos no Norte Global de uso doméstico e político das capacidades cibernéticas ofensivas, como as revelações na Espanha, Grécia, Hungria e Polônia (European Parliament, 2023). Esses casos de uso doméstico, com países integrantes da União Europeia e OTAN, reforça o argumento de que a ausência de um referente externo de securitização facilita o emprego doméstico desse tipo de capacidade.

5.2 Implicações para a ciberdefesa no Sul Global

O conjunto dos casos se contrapõe à tese do déficit cibernético do Sul Global, uma vez que esses Estados possuem e empregam capacidade cibernética ofensiva. O que os distingue dos poderes cibernéticos tradicionais está no alvo das ações, ancorados na configuração do complexo regional de segurança e na herança coercitiva da formação do Estado.

Assim, a ponderação deixa de ser o avanço da capacidade cibernética no Sul Global, mas para qual propósito ela é empregada, o que impõe reflexão sobre os programas de cooperação e de capacity-building voltados a elevar o nível técnico ofensivo, porque, na ausência de salvaguardas locais, eles podem terminar por viabilizar ações contra alvos domésticos em lugar da defesa externa.

As doutrinas de ciberdefesa no Sul Global costumam ser redigidas a partir do modelo de ameaças de referência externa, mas isso não descreve o emprego efetivo da capacidade cibernética adequadamente. Quando as doutrinas falam em defesa nacional e a prática consiste em vigilância da vida política interna, o rótulo técnico da ciberdefesa passa a funcionar como cobertura discursiva para o controle doméstico.

Disso decorre a necessidade de demarcar, no desenho institucional, a defesa cibernética militar da atividade de inteligência e da segurança pública, submetendo o emprego de ferramentas intrusivas a autorização judicial prévia e a supervisão legislativa permanente. A análise da governança de cibersegurança no Brasil aponta

na mesma direção, ao mostrar que o país securitizou o ciberespaço por meio de um conjunto amplo e desconexo de documentos, sem instrumentos claros de controle sobre o emprego das capacidades (Goldoni; Rodrigues; Medeiros, 2024).

No plano normativo, o arcabouço multilateral aceita o emprego ofensivo entre Estados, mas silencia sobre a vigilância de opositores e sobre a interrupção de conectividade contra a própria população. O Processo Pall Mall, primeiro esforço dedicado a essa face do problema, ainda não alcança os Estados que dirigem essas ferramentas contra as suas populações, e um regime que pretenda ser relevante para o Sul Global precisa incorporar a dimensão doméstica e de direitos humanos.

Outro ponto de debate a ser revisitado é a autonomia tecnológica. Apresentado pelo Sul Global como projeto emancipatório para reduzir a dependência do Norte Global, deve ser questionado se a capacidade ofensiva é comprada no mercado internacional (dominado pelo Norte Global) e utilizado contra a própria população, mantendo-se a dependência de fornecedores estrangeiros (Calderaro; Craig, 2020; Malagutti; Gama Neto, 2020).

A percepção do Sul Global como vítima da dependência tecnológica e como agente de repressão doméstica descrevem o mesmo fenômeno por ângulos distintos. Assim, os controles de exportação dos países do Norte Global devem se tornar preocupação também do Sul Global e da sua agenda de ciberdefesa. O argumento de uso doméstico - verdadeiro ou não - pode ensejar a restrição de acesso a novas tecnologias ofensivas, por vezes, num regime de controle de exportação similar ao que os Estados Unidos aplicam sobre a China no caso de inteligência artificial (CSIS, 2022).

Os resultados recomendam, por fim, uma revisão das métricas com que se avalia o poder cibernético da região. O racional convencional de *hard power* cibernético, calibrado pelas dinâmicas do Norte, não se transpõe sem mediação, o que reafirma a necessidade de um debate de segurança e defesa cibernéticas próprio do Sul Global, conduzido a partir das suas dinâmicas regionais de ameaça (Buzan; Wæver, 2003; Oliveira et al., 2017).

6 CONCLUSÃO

Este artigo comparou os casos de México, Etiópia, Brasil e Índia-Paquistão para compreender a direção do uso das capacidades cibernéticas no Sul Global. Como resultados, identificou-se que México e Etiópia, sem um rival estatal recíproco, dirigiram o emprego documentado das suas capacidades ao plano interno. O Brasil, mesmo dotado de doutrina e de ambição em defesa cibernética, repetiu o padrão. Já a Índia e o Paquistão, únicos com rivalidade recíproca estatal, manifestaram uso externo e doméstico da capacidade cibernética ofensiva. A repressão transnacional com foco doméstico, no caso etíope, reforça a tese central do trabalho que a motivação para o emprego de capacidade cibernética ofensiva reside no objeto referente.

Identificamos que dois fatores explicam esse padrão, primeiro que a configuração do complexo regional define se há um rival externo capaz de sustentar a securitização do inimigo perante a audiência interna, e a orientação histórica do estado define para onde a capacidade tende a se voltar quando não há esse rival. Onde os dois apontam para dentro, como no México, na Etiópia e no Brasil, a capacidade cibernética segue a mesma direção. Onde existe um rival recíproco, como entre Índia e Paquistão, percebe-se que isso também se torna fator para vetor externo.

Para o debate de política de segurança, o artigo corrige a tese do déficit de capacidades cibernético e desloca a discussão para o seu uso e mecanismos de controle necessários para esse processo. Novas linhas de pesquisa podem aprofundar quais critérios levam países a utilizar capacidades cibernéticas ofensivas contra alvos domésticos de modo abusivo, pois o fenômeno não está claramente situado ou delimitado de forma causal na literatura.

REFERÊNCIAS

ACCESS NOW. **Emboldened offenders, endangered communities: internet shutdowns in 2024**. #KeepItOn. [S. l.]: Access Now, 2025.

AYOOB, Mohammed. **The Third World Security Predicament: state making, regional conflict, and the international system**. Boulder: Lynne Rienner, 1995.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa**. Brasília: Ministério da Defesa, 2024.

BRUSTOLIN, Vitelio. Comparative Analysis of Regulations for Cybersecurity and Cyber Defence in the United States and Brazil. **Revista Brasileira de Estudos de Defesa**, v. 6, n. 2, p. 93-123, 2019.

BUZAN, Barry; WÆVER, Ole. **Regions and Powers: the structure of international security**. Cambridge: Cambridge University Press, 2003.

BUZAN, Barry; WÆVER, Ole; DE WILDE, Jaap. **Security: a new framework for analysis**. Boulder: Lynne Rienner, 1998.

BUZAN, Barry; HANSEN, Lene. **A Evolução dos Estudos de Segurança Internacional**, UNESP, 2012.

CALDERARO, Andrea; CRAIG, Anthony J. S. Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. **Third World Quarterly**, v. 41, n. 6, p. 917-938, 2020.

CANONGIA, Claudia; MANDARINO JUNIOR, Raphael (org.). **Livro verde**: segurança cibernética no Brasil. Brasília: GSIPR/SE/DSIC, 2010.

CENTENO, Miguel Ángel. **Blood and Debt: war and the nation-state in Latin America**. University Park: Pennsylvania State University Press, 2002.

CISCO TALOS. **Transparent Tribe campaign uses new bespoke malware to target Indian government officials**. [S. l.]: Cisco Talos Intelligence, 2022.

CNN BRASIL. Entenda o que é o FirstMile, sistema que, segundo a PF, foi usado pela Abin para espionagem ilegal. **CNN Brasil**, [s. l.], 20 out. 2023.

CSIS (Center for Strategic and International Studies). **Choking off China's Access to the Future of AI**. Washington, D.C., 2022.

DEIBERT, Ronald J. **Reset: reclaiming the internet for civil society**. Toronto: House of Anansi Press, 2020.

DEVANNY, Joe; GOLDONI, Luiz Rogério Franco; MEDEIROS, Breno Pauli. The rise of cyber power in Brazil. **Revista Brasileira de Política Internacional**, Brasília, v. 65, n. 1, e013, 2022.

EUROPEAN PARLIAMENT. **Committee of Inquiry to investigate the use of Pegasus and**

equivalent surveillance spyware (PEGA). Report on the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware. Bruxelas: European Parliament, 2023.

EVANS, Peter; RUESCHEMEYER, Dietrich; SKOCPOL, Theda (org.). **Bringing the State Back In**. Cambridge: Cambridge University Press, 1985.

FELDSTEIN, Steven. **The Rise of Digital Repression: how technology is reshaping power, politics, and resistance**. New York: Oxford University Press, 2021.

FORBIDDEN STORIES. **The Pegasus Project**. Paris: Forbidden Stories, 2021.

FORBIDDEN STORIES. Pegasus in Rwanda: sister of presidential candidate, high-ranking Rwandan politicians added to spyware list. **Forbidden Stories**, Paris, 29 maio 2024.

GEORGE, Alexander L.; BENNETT, Andrew. **Case Studies and Theory Development in the Social Sciences**. Cambridge, MA: MIT Press, 2005.

GIDDENS, Anthony. **The Nation-State and Violence**. Cambridge: Polity Press, 1985.

GOHDES, Anita R. Repression technology: internet accessibility and state violence. *American* **Journal of Political Science**, v. 64, n. 3, p. 488-503, 2020.

GOLDONI, Luiz Rogério Franco; RODRIGUES, Karina Furtado; MEDEIROS, Breno Pauli. Qual é o futuro da governança de cibersegurança no Brasil? **Cadernos Gestão Pública e Cidadania**, São Paulo, v. 29, e90972, 2024.

GREITENS, Sheena Chestnut. **Dictators and Their Secret Police: coercive institutions and state violence**. Cambridge: Cambridge University Press, 2016.

HERBST, Jeffrey. **States and Power in Africa: comparative lessons in authority and control**. Princeton: Princeton University Press, 2000.

IZYCKI, Eduardo. **Nation-state cyber offensive capabilities: An in-depth look into a multipolar dimension**. Editora Dialética, 2022.

KASPERSKY. **SideWinder targets the maritime and nuclear sectors with an updated toolset**. Securelist. [S. l.]: Kaspersky, 2025.

KREPINEVICH, Andrew F. Cavalry to computer: the pattern of military revolutions. **The National Interest**, n. 37, p. 30-42, 1994.

LOBATO, Luisa Cruz. 'South Fabricated': computing stories of Global South insecurity. **Contexto Internacional**, v. 46, n. 3, e20220055, 2024.

LOVEMAN, Brian. **For la Patria: politics and the armed forces in Latin America**. Wilmington: Scholarly Resources, 1999.

MALAGUTTI, Marcelo Antonio Oslller; GAMA NETO, Ricardo Borges. Por que o Brasil deveria adotar uma distro Linux própria? **Revista Brasileira de Estudos de Defesa**, v. 7, n. 2, p. 161-183, 2020.

MANN, Michael. The autonomous power of the state: its origins, mechanisms and results. **European Journal of Sociology**, v. 25, n. 2, p. 185-213, 1984.

MARCZAK, Bill; ALEXANDER, Geoffrey; McKUNE, Sarah; SCOTT-RAILTON, John; DEIBERT, Ron. **Champing at the Cyberbit: Ethiopian dissidents targeted with new commercial spyware**. Toronto: The Citizen Lab, University of Toronto, 2017.

MARTINS, Alexandre de Oliveira. A atividade de Inteligência nos novos documentos de Defesa do Brasil. **Revista Brasileira de Estudos de Defesa**, v. 4, n. 2, 2017.

MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco. Uma análise sobre o processo de securitização do ciberespaço. **Coleção Meira Mattos**, Rio de Janeiro, v. 13, n. 46, p. 45-66, 2019.

MÉXICO. Gobierno de la República. **Estrategia Nacional de Ciberseguridad**. Ciudad de México, 2017.

MIGDAL, Joel S. **Strong Societies and Weak States: state-society relations and state capabilities in the Third World**. Princeton: Princeton University Press, 1988.

NATIONAL CYBER FORCE. **Responsible Cyber Power in Practice**. [S. l.]: HM Government, 2023.

NUNES, Ionara Aparecida; ASSUNÇÃO, Juliana Zaniboni de; BRUSTOLIN, Vitelio. Análise estrutural das estratégias de segurança cibernética do Brasil e dos Estados Unidos. **Revista Brasileira de Estudos de Defesa**, v. 9, n. 2, p. 227-250, 2022.

NYE, Joseph S. **The Future of Power**. New York: PublicAffairs, 2011.

NYE, Joseph S. Deterrence and dissuasion in cyberspace. **International Security**, v. 41, n. 3, p. 44-71, 2017.

OLIVEIRA, Marcos Aurélio Guedes de; PORTELA, Lucas Soares. As camadas do espaço cibernético sob a perspectiva dos documentos de defesa do Brasil. **Revista Brasileira de Estudos de Defesa**, v. 4, n. 2, 2017.

OLIVEIRA, Marcos Aurelio Guedes de et al. (org.). **Guia de Defesa Cibernética na América do Sul**. Recife: Ed. UFPE, 2017.

PALL MALL PROCESS. **The Pall Mall Process: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities**. Reino Unido; França, fev. 2024.

PALL MALL PROCESS. **Code of Practice for States**. Paris, abr. 2025.

R3D (RED EN DEFENSA DE LOS DERECHOS DIGITALES). **Ejército espía: el uso de Pegasus contra periodistas y personas defensoras de derechos humanos en México**. Ciudad de México: R3D, 2022.

SCHENKKAN, Nate; LINZER, Isabel. **Out of Sight, Not Out of Reach: the global scale and scope of transnational repression**. Washington, D.C.: Freedom House, 2021.

SCOTT, James C. **Seeing Like a State: how certain schemes to improve the human condition have failed**. New Haven: Yale University Press, 1998.

SKOCPOL, Theda. **States and Social Revolutions: a comparative analysis of France, Russia, and China**. Cambridge: Cambridge University Press, 1979.

SOIFER, Hillel; VOM HAU, Matthias. Unpacking the strength of the state: the utility of state infrastructural power. **Studies in Comparative International Development**, v. 43, n. 3-4, p. 219-230, 2008.

STEPAN, Alfred. **Rethinking Military Politics: Brazil and the Southern Cone**. Princeton: Princeton University Press, 1988.

TILLY, Charles. War making and state making as organized crime. In: EVANS, Peter; RUESCHEMEYER, Dietrich; SKOCPOL, Theda (org.). **Bringing the State Back In**. Cambridge: Cambridge University Press, 1985. p. 169-191.

TILLY, Charles. **Coercion, Capital, and European States***, AD 990-1990*. Cambridge: Blackwell, 1990.

UNITED NATIONS. **Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security**. Doc. A/70/174. Nova York, 22 jul. 2015.

UNITED NATIONS. **Open-ended Working Group on developments in the field of ICTs in the context of international security: Final Substantive Report**. Doc. A/AC.290/2021/CRP.2. Nova York, mar. 2021.

US DEPARTMENT OF DEFENSE. **Summary: Department of Defense Cyber Strategy 2018**. Washington, D.C., 2018.

VILAR-LOPES, Gills. **Relações Internacionais Cibernéticas (CiberRI): uma defesa acadêmica a partir dos estudos da segurança internacional**. 2016. 171 f. Tese (Doutorado em Ciência Política) - Universidade Federal de Pernambuco, Recife, 2016.

WEBER, Max. **Ciência e política: duas vocações**. São Paulo: Cultrix, 2011.

XU, Xu. To repress or to co-opt? Authoritarian control in the age of digital surveillance. **American Journal of Political Science**, v. 65, n. 2, p. 309-325, 2021.

Autoria

1 Luiz Gustavo Lavandoski da Silva

Atua como analista e pesquisador de segurança cibernética; Doutorando em Economia Política Mundial

https://orcid.org/0000-0003-3102-6062 • silvagustavo562@gmail.com

2 Eduardo Arthur Izycki

Líder do Grupo de Estudos e Pesquisa em Segurança Internacional do Instituto de Relações Internacionais da Universidade de Brasília; Professor no Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa; Doutorando em Relações Internacionais

https://orcid.org/0000-0001-9514-7723 • eduardo.izycki@aluno.unb

Como citar este artigo

LAVANDOSKI DA SILVA, L. G.; IZYCKI, E. A. O Sul Global e o dilema da segurança: ameaça doméstica e vigilância cibernética. **InterAção**, Santa Maria, v. 17, n. 3, e98413, p. 1-32, 2026. DOI 10.5902/2357797598413. Disponível em: https://dx.doi.org/10.5902/2357797598413. Acesso em: dia mês abreviado. ano.