# Ciberdefesa e *software power*: uma análise exploratória da China

## Cyberdefense and software power: an exploratory analysis of China

Rev. Bras. Est. Def. v. 11, n. 1, jan./jun. 2024, p. 181–204
DOI: 10.26792/RBED.v11n1.2024.75323
ISSN 2358-3932

**BRUNO MOSER NUNES**
**THAYS FELIPE DAVID DE OLIVEIRA**
**RENATO VICTOR LIRA BRITO**

## INTRODUÇÃO

O desenvolvimento tecnológico e internético trouxe às relações internacionais um novo espaço, o espaço cibernético, e uma nova dinâmica, na qual os Estados passaram a exercer seus poderes, particularmente o *Software Power*. Não obstante, este novo espaço ainda está em expansão e disputa pelos Estados, e possui uma complexidade que todavia está sendo descoberta e pressionada por novas formas de ameaças nacionais e internacionais.

Neste sentido, o objetivo geral deste trabalho é compreender se esta forma de poder, *o Software Power*, é utilizada nos moldes tradicionais de proliferação, ou seja, como uma ferramenta para manifestar os interesses estatais e atingir seus fins soberanos; ou se sua utilização se dá de forma independente e isolada daquelas que comumente atuam através da coerção (*hard power*) ou do convencimento (*soft power*). Para alcançar este objetivo,

**Bruno Moser Nunes** é doutor em Ciências Sociais pela Faculdade Latino-Americana de Ciências Sociais/Argentina (Flacso Argentina) e mestre em Relações Internacionais pela Universidade Federal de Santa Catarina (UFSC). **Contribuição no artigo:** Colaboração conjunta na redação e na análise do artigo. orcid.org/0000-0001-6236-2785. E-mail: brunomosernunes@hotmail.com.
**Thays Felipe David de Oliveira** é doutora em Ciência Política pela Universidade Federal de Pernambuco (UFPE) e mestra em Antropologia pela Universidade Federal da Paraíba (UFPB). **Contribuição no artigo:** Colaboração conjunta na redação e na análise do artigo. orcid.org/0000=0002-7317-5704-?lang-en. E-mail: thays.felipe@ufpe.br.
**Renato Victor Lira Brito** é doutorando e mestre em Ciência Política pela Universidade Federal de Pernambuco (UFPE). É editor-executivo da *Revista Política Hoje*. **Contribuição no artigo:** Colaboração conjunta na redação e na análise do artigo. orcid.org/0000-0001-6012-8469. E-mail: renato.lirabrito@ufpe.br.

analisaremos de forma exploratória a estratégia da China neste âmbito da ciberdefesa, a partir de seus documentos oficiais, buscando entender seu pensamento, bem como seu orçamento, diretrizes, objetivos estratégicos e mecanismos chineses em sua relação com o Espaço Cibernético.

Tomando por base a conceitualização teórica proposta por Vilar-Lopes (2017) e Ventre (2011), entendemos que o *Software Power* é aquela forma de poder que se expressa através de programas, sistemas, aplicativos e informações naquelas estruturas físicas e virtuais que compõem o espaço cibernético. Este *Software Power* implica em respostas às novas preocupações geopolíticas para a defesa dos Estados e a segurança de seus cidadãos, no que se refere à proteção de dados, estratégias militares e ao fluxo da informação.

Este estudo utiliza uma metodologia qualitativa para explorar analiticamente o tema por meio de uma análise exploratória sobre o conceito de *Software Power* através do estudo do caso Chinês (Sátyro and D'Albuquerque 2020). Para tanto, nos dedicamos a uma análise da discussão teórica que permeia o objeto da pesquisa, e também sobre as diferentes conceitualizações de estratégias de expansão de poder. Em seguida, realizamos a análise do caso chinês e da sua relação com o *Software Power* e o espaço cibernético.

## O ESPAÇO CIBERNÉTICO

Em virtude do avanço da tecnologia e da Internet desde meados do século passado, observamos um crescente interesse político, acadêmico e social em entender o espaço cibernético e as questões relacionadas a essa temática, para além dos que já foram tratados nas áreas da Ciência da Computação, Sistemas de Informação e afins. De tal forma, em Relações Internacionais e na Ciência Política notamos um aumento no número de pesquisas que envolvem o espaço cibernético e, mais especificamente, aquelas questões ligadas à Defesa Nacional e à geopolítica.

Para Clarke (2012), esse território pode ser constituído por aspectos tangíveis e intangíveis. De forma complementar, ele ainda define o espaço cibernético como toda a rede de computadores contidos no mundo, ou seja, todas as coisas que estão conectadas a tais aparelhos ou que de alguma forma estão submetidas aos seus controles.

No entanto, o *Glossário das Forças Armadas* entende o espaço cibernético como "Espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas." (Brasil 2015, 106), que é a definição utilizada por nós.

Para Ventre (2011) o espaço cibernético é consequência da soma de três camadas elementares: *hardware*, *software* e *peopleware*. Essa composição nos permite definir esse território como um conjunto de equipamentos físicos (*hardware*) que sustenta uma dimensão virtual com programas, sistemas, aplicativos e informações (*software*), cuja manipulação se dá por uma camada cognitiva de usuários (*peopleware*).

Desta forma, o Espaço Cibernético não é natural como aqueles tradicionais que já são conhecidos; entretanto, este foi um ambiente criado pela própria sociedade (Portela 2015, 94). Nesse sentido, ele é um território que se diferencia dos demais no que diz respeito à interconectividade, tendo em vista que transpassa todos os supracitados, podendo atingir os territórios aéreo, terrestre e marítimo (Ventre 2011, Lira-Brito 2020; 2023, and Lanzetta 2023). Vejamos a Figura 1, a seguir, para compreender de forma clara a relação entre o espaço cibernético com os demais espaços geográficos:

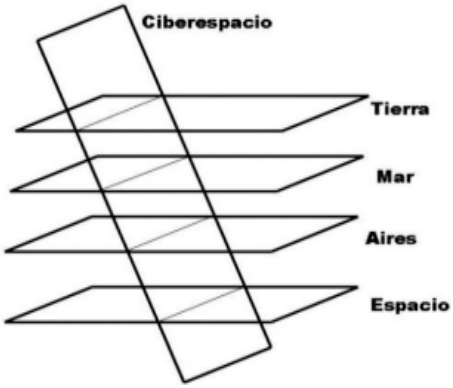


Figura 1 — Relação do Espaço Cibernético com os demais espaços geográficos.
Fonte: Ventre (2012) *apud* Portela (2015).

O Espaço Cibernético possui a característica da transversalidade, já que passa por todas as dimensões convencionais de domínio: terra, ar, mar e espaço (Ventre 2012 *apud* Toso 2016, 463). Deste modo, constitui uma nova face de poder, que procura ser acumulada pelas grandes potências mundiais.

Em virtude do panorama anterior, os países, há pouco mais de uma década, começaram a se preocupar com essas ameaças, percebendo a necessidade de formular uma proteção de infraestrutura de dados, da defesa

do Estado, entre outros descritores (Hathaway 2015). Disto se deriva que a maioria dos governos têm aumentado as capacidades defensivas existentes de seus órgãos de segurança, defesa e inteligência, particularmente dentro de sua estrutura militar (Lewis and Timlin 2011). Neste sentido, a principal área da estratégia nacional que revela a preparação cibernética de um país é "a articulação e publicação de uma Estratégia Nacional de Cibersegurança que alinhe a visão econômica do país com seus imperativos de segurança nacional" (Hathaway 2015, 6–7).

O avanço sobre os estudos do Espaço Cibernético nas Relações Internacionais, atualmente se dá, sobretudo, em seu aspecto securitário (Teixeira Junior, Vilar Lopes and Freitas 2017; Portela 2015). Na perspectiva do debate sobre transformações na conduta da guerra, as ideias de "redução da fricção" e "distanciamento do front" (Peron 2016) são a ponta de lança da chamada Revolução dos Assuntos Militares (RAM), como afirmado por Teixeira Júnior, Vilar Lopes e Freitas (2017, 31):

> Com a substituição de sistemas analógicos por digitais, a incorporação da computação nos sistemas de comando e controle (C2) e a eficiência produtiva do capitalismo ocidental, a nova revolução tecnológica empurrava o mundo à era da informação, com profundos impactos também na arte da guerra. Por exemplo, a internet, surgida no contexto da Guerra Fria, passa ao domínio público ainda nos anos de 1980 e se populariza nos de 1990, quando a luta contra as ameaças cibernéticas toma dimensões políticas. Emergia lentamente um novo paradigma de combate, característico dessa nova era, a *information warfare*.

A forma com que o Espaço Cibernético permite o avanço de conquistas e interesses estatais sem uma grande exposição, faz com que os Estados se utilizem desse meio para projetar poder. Desta maneira entramos numa discussão já sacramentada na área das Relações Internacionais, mas que merece uma atenção especial: o poder e a projeção de poder.

## Poder e projeção de poder

Antes das grandes guerras, era bastante comum as pessoas associarem o termo poder ao contingente bélico, mas mudanças na sociedade internacional tornaram o poder um conceito polissêmico, não apenas militar. Segundo Nye (2009, 74) "Poder é a capacidade de alcançar as próprias propostas e metas. Mais especificamente, é a capacidade de afetar os outros para obter os resultados desejados". Ou seja, poder é a capacidade de proliferar o interesse e fazer com que outros o adotem como seus.

Nye (2009, 76) argumenta que "um país é capaz de alcançar seus resultados desejados no mundo da política porque outros países querem imitá-lo ou concordam com um sistema que produza tais efeitos". Desta maneira, o poder pode ser projetado de forma suave ou violenta, conhecidas como *Soft Power* e *Hard Power*.

Morgenthau (2003), afirma que os governantes dos Estados agem de forma racional e amoral na política internacional, direcionando suas escolhas políticas na busca por: manter o poder, mediante preservação do *status quo*; aumentar o poder, por meio do imperialismo; ou demonstrar o poder, via diplomacia ou projeção de força (Vilar-Lopes 2017). Interessa a esta pesquisa esta última forma de projeção de poder, a qual se encaixa na discussão sobre o espaço cibernético. Para Morgenthau (2003):

> A aspiração de poder por parte de várias nações, em que cada uma tenta manter ou alternar o *status quo*, leva necessariamente a uma configuração que é chamada de equilíbrio de poder, bem como as políticas que se destinam a preservar esse equilíbrio. [...] O equilíbrio internacional de poder representa apenas uma manifestação particular de um princípio social de ordem geral, ao qual todas as sociedades compostas de um certo número de unidades autônomas devem a autonomia de suas partes componentes. [...]. Existem dois pressupostos na base de todas essas formas de equilíbrio: que os elementos a serem equilibrados são necessários para a sociedade ou têm direito de existir; e segundo: que, sem um estado de equilíbrio entre eles, um dos elementos ganhará ascendência sobre os demais, desrespeitará seus interesses e direitos e poderá finalmente destruí-los. (Morgenthau 2003, 321).

É de grande importância analisar a questão do equilíbrio de poder no sistema internacional anárquico porque, ao entendermos os Estados como atores soberanos, devemos buscar compreender seus comportamentos frente a esta estrutura ausente de um poder central regulador. A projeção de poder em um ambiente anárquico é o *modus operandi* de sobrevivência dos Estados no cenário internacional; é a forma que os governantes juntos aos países encontram de dissuadir outros atores.

Bull (2002), a partir da teoria da Escola Inglesa, referente ao Sistema Internacional, nos apresenta a ideia da sociedade anárquica. A partir da ideia hobbesiana do Leviatã, ente que poderia ditar as regras de conduta entre os agentes, o autor afirma que sua ausência (Leviatã) implicaria em conviver sob a influência de muitos constrangimentos internacionais. Esse vácuo de poder supranacional gera incentivos para os Estados usarem outros métodos, que não os tradicionais, para projetarem poder (Vilar-Lopes 2017).

Dentre outros métodos está a possibilidade da utilização do espaço cibernético para manifestação e proliferação do poder. Vilar-Lopes (2017) dá a esta utilização o nome de *Software Power*. Em linhas gerais, seria a utilização do espaço cibernético, por meio dos *softwares* para a manifestação do poder.

> Daí, acredita-se, advém a necessidade de avaliar o impacto tecnológico das ameaças, vulnerabilidades e estabilidades/instabilidades estratégicas. O ciberespaço não foge à risca dessa observação, constituindo-se ora como meio, ora fim, ora nível de análise cuja unidade básica é o *software*. É na junção dessas três percepções que se concentra o conceito de *Software Power* (Vilar-Lopes 2017, 7).

A preocupação desta pesquisa perpassa o conceito criado por Vilar-Lopes (2017) — não no que tange a originalidade e consistência do conceito, e sim à utilização do *Software Power* no cotidiano do Estado. Cabe-nos, nesta pesquisa, compreender se o chamado *Software Power* é utilizado para a proliferação de poder nos moldes tradicionais, servindo, portanto, como uma peça para manifestação dos interesses estatais; ou se a utilização se dá de forma independente, sendo assim uma manifestação de poder isolada.

## A projeção de poder no espaço cibernético

O conceito de *Software Power* traz consigo uma terceira via de projeção de poder no sistema internacional ao lado dos conceitos de Hard Power, Soft Power e Smart Power (Vilar-Lopes 2017). O *Software Power* se volta sobretudo a questão do Espaço Cibernético, diferenciando-se do conceito de *Cyberpower* antes criado por Nye (2011):

> [...] conjunto de recursos relacionados à criação, controle e comunicação da informação eletrônica e computacional – infraestrutura, redes, *softwares* e habilidades humanas, incluindo não apenas a rede mundial de computadores, mas também intranets, tecnologias móveis e comunicações espaciais (Nye 2011, 123, tradução nossa).[1]

O conceito criado por Vilar-Lopes (2017) tem como objetivo analisar como os Estados se utilizam do *software*, um dos objetos que compõem o espaço cibernético, para projetar poder. Neste trabalho, entretanto, optamos por não focar a nossa análise no que inicialmente apresentamos como *Hardware* e *Peopleware*. As preocupações atuais, tanto ao nível da esfera da Administração Pública Federal quanto ao nível da esfera privada, se direcionam hoje ao *software* (Vilar-Lopes 2017).

> O conceito de Cyberpower não consegue, arrisca-se a dizer, exprimir, com maior grau de acurácia, o elo intrínseco entre o ciberespaço

> e a projeção/obtenção de poder na política internacional, muito mais concernente às relações internacionais do que a difusão de poder. Portanto, esse conceito nyeiano preocupa-se, de forma precípua, em explicar (i) como o poder, travestido de informação, é difundido no ambiente cibernético – especialmente na Internet – e, por conseguinte, (ii) como isso se torna um desafio para o Estado-nação. (Vilar-Lopes 2017).

O presente trabalho busca avançar e analisar fatos para além do que era o objetivo de Joseph Nye. Assim como foi elaborado por Teixeira Junior, Villar-Lopes e Freitas (2017), em um trabalho com questionamentos em relação ao Espaço Cibernético no que diz respeito à guerra, esta pesquisa também intenciona analisar como os Estados se utilizam do espaço cibernético para projetar poder.

Liles et al. (2012) tratam a questão de a literatura não abrir espaço para afirmações se a guerra cibernética é o uso do espaço cibernético como domínio para o combate (Birdwell and Mills 2011) ou é o próprio combate no domínio do Espaço Cibernético (Libicki 2012). Perante o exposto, é necessário compreender como o *Software Power* representa o uso do espaço cibernético como domínio para projetar poder de forma independente, ou se este é uma arma para projetar poder em termos tradicionais.

## A CHINA NO ESPAÇO CIBERNÉTICO: CIBERDEFESA E PROJEÇÃO DE PODER

Na seção que se apresenta, a partir de fontes documentais, busca-se fornecer informações valiosas sobre a configuração do pensamento estratégico chinês no marco do espaço cibernético para tratar a projeção de poder.

Segundo Hathaway (2015, 2), a China considera a Internet como uma chave para suas futuras oportunidades de crescimento e desenvolvimento. Diversos autores (Hong and Goodnight 2019; Herold 2011; Denardis 2014) tratam da promoção da China na busca da soberania cibernética ao desenvolver tecnologias da informação e da comunicação que reforçam os debates sobre a projeção de poder no Espaço Cibernético. Assim, na ausência de instituições globais autorizadas, os Estados desenvolvem, no âmbito doméstico, marcos regulatórios da Internet, mas também diferentes modos de governança cibernética em escala global.

A postura da China em governança cibernética marca uma maneira diferente de pensar a práxis, mas não deve ser vista como um relacionamento binário com o Norte Global ou o Ocidente, e sim como composta por relações de poder históricas, geopolíticas e epistemológicas (Wasserman

2018). Neste sentido, o espaço cibernético chinês foi convencionalmente produzido no imaginário territorial do Estado (Shen 2017). Ao retratar uma relação de disputa e conquista entre o Estado preocupado com a insegurança do regime e dos prováveis usos sociais variados, a regulação e fiscalização implicitamente enquadram a Intranet chinesa contra a internet global (King, Pan, and Roberts 2013; Rauchfleisch and Schäfer 2015). Com isso, o espaço cibernético chinês é pautado pela projeção de poder do Estado e da manutenção das estruturas estatais. A eficácia do controle estatal legitimou a implantação do *Great Firewall* como uma política de governança da Internet na China (Mackinnon 2011).

Segundo Hong e Goodnight (2019), a proposta de soberania cibernética chinesa também serve para institucionalizar a projeção de poder cibernético do Estado chinês. A prática do discurso e da política afirmam o poder estatal em todas as esferas do espaço cibernético da China nacionalmente, mas também induzem a China a uma posição reativa no espaço cibernético global.

A China já possuía a maior população de usuários da Internet no mundo em 2018 (CNNIC 2018). O crescimento histórico único das infraestruturas de rede, bem como a criação de uma indústria nacional de Internet doméstica, levou à criação do campo de pesquisa chamado de Estudos Chineses da Internet. De acordo com Negro (2019), a principal narrativa é de que a China é um país de defesa em seu campo cibernético e que a Intranet chinesa permitiu ampliar o controle do Estado. O governo chinês impõe maior controle sobre as redes internas, tanto para suprimir a oposição doméstica quanto para bloquear e proteger o sistema de ameaças externas. Para isso, cercou o país com o *Great Firewall*, também conhecido como Projeto Golden Shield, que é um projeto de vigilância da Internet operado pelo Ministério de Segurança Pública (Ministry of Public Security — MPS). A eficácia das ciber-unidades chinesas deve-se à estreita cooperação entre estruturas governamentais, militares e *hackers* (NO 2017). O governo chinês mantém os programas de controle de dados e informações com a justificativa de benefícios sociais, políticos e econômicos para sua população.

> [...] dominar as técnicas de redes de comunicações e tecnologia, bem como obter informações úteis para a nação, tendo como campo o ciberespaço. De acordo com autoridades chinesas, pode criar empregos, elevar o padrão de vida da população, acelerar o desenvolvimento de regiões atrasadas, formar um nova nação progressista da China, o que significa fazer da China um poder autossuficiente e ajudá-la a assumir posições de liderança no mundo em todas as esferas da vida. (Ibragimova 2017).

Desse modo, a projeção de poder da China consiste em todo o aparato tecnológico e informacional doméstico que possibilita sua organização de dados, defesa e projeção no ambiente cibernético global. Nesse sentido, o governo da China desenvolve uma política de segurança cibernética que promove a estabilidade do seu ambiente cibernético e atua em sua manutenção de poder, no âmbito doméstico, e na projeção de poder defensivo, em âmbito internacional.

A estruturação e implementação de uma política de ciberdefesa permite que a percepção dos riscos enfrentados e suas repercussões sejam traduzidas em medidas a serem implementadas. Por sua vez, "facilita a adoção de uma atitude preventiva e reativa em relação aos problemas de segurança e permite reduzir riscos e suas repercussões" (UIT 2009, 11).

A característica essencial da política chinesa de ciberdefesa é que "sua atividade cibernética é impulsionada principalmente pelo imperativo político nacional de proteger a longevidade do Partido Comunista Chinês" (PCC) (Chang 2014, 7). Neste sentido, tanto sua política nacional quanto o seu desenvolvimento militar nos últimos anos indicam que ambos os campos da cibersegurança e da ciberdefesa são de alta prioridade para o governo chinês (Chang 2014, 8).

> O discurso de Xi Jinping na primeira reunião da *Central Network Security and Informatization Leading Small Group* (中央 网络 安全 和 信息 化 领导 小组, *zhongyang wangluo anquan ele xinxihua Lingdao Xiaozu*) em 2014 marcou um novo e alto nível de priorização cibernética como uma importante iniciativa estratégica com implicações políticas, econômicas e militares, e também indicou a importância relativa da segurança da rede na agenda política chinesa. O discurso de Xi também apontou que o governo central percebe a segurança de redes e informações como dois componentes principais de segurança doméstica e desenvolvimento nacional". (Xi Jinping *apud* Chang 2014).

Assim sendo, entre as primeiras diretrizes de estratégia militar que orientaram a política de ciberdefesa chinesa, destacam-se:

1. A "Guia Estratégica Militar" (1956; 1980; 1993), cujo conteúdo explica as prioridades e objetivos estratégicos na modernização, estrutura e organização da força, além de fornecer informações sobre como o Exército de Libertação Popular (ELP) entraria em guerra.
2. "O Documento 27"[2] do Conselho do Estado do ano de 2003, que delineou a estratégia nacional de segurança de redes civis e segurança de informações da China;

3. A "Estratégia Nacional de Desenvolvimento da Informatização, 2006-2020",[3] promulgada pelo Comitê Central do Partido Comunista e o Conselho de Estado, a qual ressalta a necessidade de aumentar o investimento na proteção dos sistemas de informação do governo; "A Ciência da Estratégia Militar" do ano de 2013, que descreve o pensamento estratégico sobre como o PLA se prepararia para impedir e batalhar a guerra;
4. O "Livro Branco da China"[4] do ano de 2013, que trata do emprego diversificado das Forças Armadas da China;
5. A "Resolução sobre o fortalecimento do trabalho de segurança da informação" do ano de 2014, o qual enfatiza o desenvolvimento de recursos cibernéticos sob a perspectiva de "defesa ativa"[5] (Hathaway 2015). É dizer que, segundo o conteúdo destes documentos, o Exército Popular de Libertação não atacará a menos que seja atacado, mas se for atacado, ele reagirá no espaço cibernético.
6. Outras destas diretrizes baseiam-se nas "Regras de Conduta na Área de Segurança da Informação", publicadas em 2015 pela OCX (Organização de Cooperação de Xangai),[6] onde são detalhadas as diretrizes para tratar da cibersegurança e da ciberdefesa. Este documento descreve o objetivo da proposta, que é identificar os direitos dos Estados no ciberespaço, promover e criar um comportamento responsável nele. Além do mencionado, estas regras buscam a cooperação para a solução de problemas semelhantes nas tecnologias da informação e comunicação, a fim de facilitar o desenvolvimento social e econômico, bem como o bem-estar das pessoas, garantindo a paz e a segurança (Unga 2023, 4).

Por sua vez, o governo chinês tem adotado uma série de novas leis, nomeadamente a "Lei de Segurança do Estado", adotada em 1º de julho de 2015, a "Lei Antiterrorismo", a "Lei da Cibersegurança", a "Lei relativa à gestão das ONG estrangeiras" e a "Lei chinesa de cibersegurança",[7] que entrou em vigor em 1º de junho de 2017. Estas novas leis implementam o pensamento do Presidente Xi Jinping de que "sem segurança cibernética não há segurança nacional". No entanto, seu conteúdo está dotado de uma alta censura e controle sobre a Internet e as transações comerciais, a tal ponto, que "o ativismo público e as críticas pacíficas ao governo são consideradas como ameaças à segurança do Estado" [...];[8] e "a regulamentação a respeito de empresas tecnológicas tem ganhado a rejeição internacional, pois interfere indevidamente nas relações comerciais".[9]

No entanto, a primeira estratégia formal no marco internacional de aplicação cibernética da República Popular da China consiste na "Estratégia

Internacional de Cooperação no Espaço Cibernético", de data relativamente recente, publicada apenas em março de 2017. O texto é muito semelhante às Regras de Conduta sobre Segurança da Informação supracitadas. Seu conteúdo define os objetivos do governo chinês em termos de segurança cibernética, cooperação internacional e como busca exercer seus objetivos de ciberdefesa (Schreiber 2019). O objetivo estratégico da participação da China no âmbito internacional do espaço cibernético se compõe de seis dimensões:

> (1) salvaguardar resolutamente a soberania do país, os interesses de segurança e desenvolvimento no ciberespaço; (2) garantir um fluxo seguro e ordenado de informações na Internet; (3) melhorar a conectividade global; (4) manter a paz, segurança e estabilidade no ciberespaço; (5) melhorar o estado do direito internacional no ciberespaço; promover o desenvolvimento global da economia digital; e (6) aprofundar o intercâmbio cultural e a aprendizagem mútua, para que os frutos do desenvolvimento da Internet cheguem a todos os cantos do mundo e beneficiem as pessoas em todos os países. (Shaohui 2017).

Perante os objetivos estratégicos da China, é evidente a possibilidade de ações com respeito às dimensões citadas, como a proteção da soberania e da segurança no espaço cibernético, que indiquem e reafirmem a posição do Estado contra qualquer interferência supranacional com os regulamentos no espaço cibernético nacional.

É para este fim que o exército chinês entende que a responsabilidade de defesa do espaço cibernético se enquadra. Portanto, sua tarefa se limita ao desenvolvimento e aprimoramento das capacidades tecnológicas no espaço cibernético e à maior participação internacional, para evitar qualquer interferência, assim como promover ações de ciberdefesa e a garantia de um fluxo seguro e ordenado de informações e dados na Internet.

No que diz respeito aos compromissos internacionais que o governo chinês reconhece no marco das suas atuações, observam-se: melhorar a conectividade global; a promoção de uma governança global multilateral no nível internacional; e a busca pela manutenção da paz, segurança e estabilidade no espaço cibernético. Ou seja, a China promove no discurso o livre trânsito de informações, desde que os interesses públicos e nacionais estejam protegidos (Shaohui 2017; Schreiber 2019). Com isso, demonstra-se a consolidação das dimensões do pensamento estratégico chinês no que tange à cooperação internacional no espaço cibernético como estratégia de ciberdefesa (ver Quadro 1).

Quadro 1
Pensamento Estratégico da Cooperação Internacional chinesa no Espaço Cibernético.

| Objetivos estratégicos | Mecanismos |
|---|---|
| Soberania digital => Soberania democrática | Prevenção do terrorismo, separatismo e extremismo |
| Controle sobre o fluxo de informações e fluxo livre de informações | Estabelecimento e coordenação de órgãos regionais de combate ao terrorismo |
| Contra interferências nos assuntos de outro Estado | Salvaguardar a soberania no espaço cibernético |
| Proteger as liberdades e os direitos dos cidadãos no espaço cibernético | Governança global justa e transparente |
| Transparência e desenvolvimento no campo do espaço cibernético | Fluxo livre de informações sob parâmetros chineses |
| Proteger informações e infraestrutura crítica que podem ser afetadas no espaço cibernético | Contra interferências nos assuntos de outro Estado |

Fonte: Modelo ajustado de Schreiber (2019).

Finalmente, pode-se dizer que houve avanços significativos nas políticas de ciberdefesa da China nas últimas duas décadas, quando novos planos e estruturas institucionais foram estabelecidos. Por outro lado, os regulamentos legislativos, que auditam e controlam o campo do espaço cibernético nacional foram rapidamente concluídos como resultado do rápido crescimento econômico e tecnológico experimentado pela China. Na atualidade, a China alcançou a posição de superpotência global, que pode dominar o campo do espaço cibernético, juntamente com os Estados Unidos e a Federação Russa (Daricili and Özdal 2017 *apud* Daricili and Özdal 2018).

Em termos gerais, a estratégia chinesa no campo cibernético pode-se reduzir a três componentes principais de seus objetivos econômicos, políticos e militares. O Quadro 2 apresenta essas características.

Quadro 2
A estratégia chinesa no espaço cibernético

| Objetivos | |
|---|---|
| 1. Econômicos | 1a) Manter o crescimento econômico e a estabilidade. |
| 2. Políticos | 2a) Proteger o poder do governo do Partido Comunista Chinês através do controle da informação, propaganda e direcionamento de fontes domésticas de possíveis distúrbios;<br>2b) Usar operações de redes de computadores para sinalizar insatisfação com potências estrangeiras por desenvolvimentos fora da China que afetam negativamente sua reputação. |
| 3. Militares | 3a) Preparar-se para cenários militares e garantir a superioridade militar em caso de conflito cibernético com um adversário por meio da modernização militar, investigação de operações de redes de computadores e cultivo de capital humano;<br>3b) Estudar e entender as infraestruturas militares, motivações, objetivos, capacidades e limitações de possíveis adversários no domínio cibernético;<br>3c) Avançar em narrativas alternativas de controle governamental sobre manipulação da cibersegurança nos níveis internacional e nacional. |

Fonte: Elaboração própria a partir de Chang (2014, 8) e Daricili and Özdal (2018, 4–5).

## Orçamento de defesa e projeção de poder

Desde o início da década de 1980, a China vem investindo pesadamente na modernização do Exército de Libertação do Popular (ELP),[10] que é o principal segmento das Forças Armadas chinesas (Dornelles Jr. 2014). No entanto, embora tenha havido muitos pedidos de maiores recursos dedicados às forças armadas, os principais líderes do ELP têm cumprido consistentemente a linha do Partido Comunista Chinês na questão da subordinação da defesa ao desenvolvimento econômico nacional. Segundo Blasko (2006, 9), como resultado de sua obediência à linha do partido, o ELP, na última década, tem aumentado seu orçamento de defesa à medida que a economia chinesa continua crescendo, pois a China busca investir em melhorias para o seu efetivo, mesmo entendendo que as despesas mencionadas acima são necessárias.

> O *International Institute for Strategic Studies* (IISS) estima que os gastos militares totais da China totalizem 1,41 bilhões de RMB (US$ 209 bilhões) em 2017. Isso inclui o orçamento central e local da defesa, compras de armas estrangeiras, estimativas de pesquisa e desenvolvimento de defesa (I+D) e o orçamento central do ELP. Levando em consideração esses itens orçamentários adicionais, os gastos de

> defesa da China na última década parecem estar em torno de 1,7 a 1,8% do PIB, em vez dos 1,2 a 1,3% oficiais. Isso representa 35% adicionais de desembolsos militares, além do número oficial (Béraud-Sudreau 2019)

Nesse sentido, os dados de 2019 estimam que o orçamento da Defesa do Estado chinês é em torno de 1,7% do PIB. Isso demonstra que o país vem investindo cada vez mais nessa área, visando assim a uma maior projeção de poder, conforme pode ser visto no Gráfico 1. Como é escassa a existência de bancos de dados que sistematizem as informações sobre os investimentos nos setores cibernéticos dos países, utilizamos, seguindo a indicação da literatura (Kremer 2014; Lira-Brito 2022), o orçamento de Defesa geral como uma *proxy* desses dados.

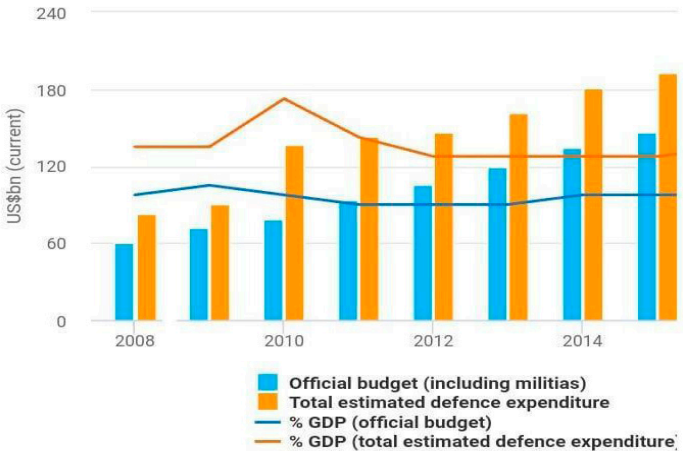


Gráfico 1. Orçamento oficial de defesa versus despesa total, 2010-2017 (US$ bi). Fonte: Béraud-Sudreau (2019).

Atualmente, o gasto em defesa da China é o segundo maior do mundo, apenas atrás dos Estados Unidos.[11] A China busca desenvolver fortes capacidades cibernéticas para proteger as redes e defender a conquista da "superioridade do espaço cibernético chinês" usando operações cibernéticas ofensivas e defensivas para impedir a capacidade de um adversário realizar operações militares contra o Estado chinês.

> [...]. Foi assim que, em dezembro de 2015, o ELP estabeleceu uma nova força de apoio (*People's Liberation Army Strategic Support Force*, PLASSF) como parte de reformas mais amplas da modernização. No

> entanto, embora muitas de suas funções e atividades permaneçam secretamente envolvidas, acredita-se que essa nova força seja responsável por facilitar a integração das capacidades de guerra do ELP no espaço, no ciberespaço e no espectro eletromagnético (EM). [...]. Acredita-se que o PLASSF compreenda várias divisões. Isso inclui o Departamento de Sistemas Espaciais, que fornece suporte espacial e informações de inteligência para os comandos recém-estabelecidos do ELP e permite futuras operações conjuntas para a projeção de poder. Por outro lado, o Departamento de Sistemas de Rede é responsável por gerenciar os recursos da guerra cibernética, eletrônica e psicológica.[12]

O recente relatório de defesa (Military and Security Developments Involving the People's Republic of China, 2019) indica que a China está focada em informação cibernética e operações no espaço cibernético. Apesar de sua posição pública contrária, é reconhecido que a China vem investindo na militarização deste espaço, tanto no combate à intervenção de *hackers* quanto no aprimoramento das operações para estabelecer uma vigilância em tempo real, aumentando a capacidade de seus sistemas.

Quanto à projeção de poder, em diferentes momentos, autoridades chinesas vêm demonstrando sua ambição de longo prazo de tornar a China uma grande potência do espaço cibernético, contando com um universo de 800 milhões de usuários chineses de internet. Além disso, tornar longeva a duração e a influência do Partido Comunista Chinês parece ser o principal objetivo de defesa da China. Para alcançar esta ambição, diferentes estratégias da chamada *China's Great Firewall* têm sido colocadas em prática pela Administração do Espaço Cibernético da China (CAC em inglês), desde o bloqueio ao acesso de *big techs* estadunidenses tais como *Google*, *Twitter*, *Youtube*, *Wikipedia* e *Meta*, até a censura à liberdade de expressão de usuários chineses e disputas pela instalação da rede 5G e seus equipamentos no mundo.[13]

Neste sentido, o governo chinês se sente sob ataque e busca promover uma expansão ordenada da internet, protegendo a reputação do PCC e os dados de cidadãos chineses, cujo direito de privacidade é considerado por Pequim um direito coletivo e não individual. Isto, por sua vez, tem implicado em limites e a verificação de pedidos de listagem de empresas chinesas em Bolsas de Valores estrangeiras e o controle de algoritmos de tecnologia, assim como multas ou suspensão de aplicativos que possam armazenar dados de usuários ou transmitir conteúdo sexual, além de plataformas de *streaming*, *video games*, educação particular, entre outros segmentos.

Por outro lado, até o momento, o governo chinês não parece visar a uma expansão internacional do seu *Software Power* cibernético para além

da tecnologia 5G, razão pela qual se restringe em termos de capacidades e possibilidades extraterritoriais. Assim sendo, a estratégia da China aponta para uma expansão de poder que se concentra principalmente em preocupações defensivas, questões internas de regulação e no desenvolvimento de uma tecnologia nacional que iniba a concorrência com empresas estrangeiras. Neste âmbito, o excesso de regulação, intervenções e multas a *big techs*, tanto da própria China quanto na China, passou a afastar investidores estrangeiros em 2022, o que tem levado o governo chinês a adiar, aliviar e revisar estas medidas, buscando estimular a sua economia, que tem demonstrado desaceleração.[14]

Em suma, contrapondo o *Software Power* chinês às formas tradicionais de expansão de poder, sejam elas pela força/coerção material (*hard*) ou pelo convencimento imaterial (*soft*), observa-se que não há uma estratégia clara da política externa chinesa para impor ou convencer outros países sobre estes programas, aplicativos, sistemas e informações oriundos da China. Por outro lado, são identificados interesses, preocupações e questões internas para a defesa chinesa e sua blindagem às influências externas no espaço cibernético.

## CONSIDERAÇÕES FINAIS

Um novo espaço de poder, o espaço cibernético, que se caracteriza por uma complexidade e transversalidade de dimensões convencionais de domínio, está em constante descoberta e disputa por parte de um conjunto de atores, dentre os quais os Estados são os principais *players*, sendo os reguladores do mundo virtual.

Neste contexto, o que se sabe sobre a China em matéria de ciberdefesa está no seu discurso ou a partir de manuais de ampla divulgação dos princípios chineses, uma vez que dados e investimentos reais em ciberdefesa são sigilosos e/ou não divulgados completamente. Portanto, esta pesquisa se concentrou em demonstrar a visão chinesa sobre projeção de poder e ciberdefesa, com ênfase no governo do PCC, que detém o poder sobre as estratégias de defesa do país no espaço cibernético.

Através de uma análise exploratória, observamos que a expansão de poder chinesa no espaço cibernético parece se diferenciar daquelas tradicionais, que se expressam pela coerção (força militar) e/ou pelo convencimento (diplomacia, entre outras). Tanto porque os principais interesses e objetivos chineses de ciberdefesa parecem ser internos, quanto porque suas preocupações com a blindagem de possíveis ameaças externas parecem ser mais um objetivo de defesa do que de política externa *per se*.

Neste sentido, no âmbito interno, a China busca manter a reputação e o *status quo* do PCC e blindar sua sociedade do acesso de *big techs* estrangeiras em solo chinês, o que termina isolando os chineses do resto do globo em termos de acesso à pluralidade de informações. Já no âmbito externo, a China limita sua expansão de poder a disputas pela instalação da rede 5G de internet e seus equipamentos, sem recorrer à força/coerção do poder militar (*hard power*) ou ao convencimento por parte da diplomacia (*soft power*).

Finalmente, a despeito de ser um tema relativamente recente em Relações Internacionais e das limitações no que se refere às fontes de materiais provenientes da China, esta pesquisa abre um leque de questionamentos para futuros estudos com respeito aos resultados que o gigante asiático vem conseguindo consolidar na sua estratégia de ciberdefesa, como, por exemplo: por quanto tempo a China conseguirá manter a reputação do PCC no espaço cibernético e restringir seus cidadãos ao acesso às empresas tecnológicas e cibernéticas estrangeiras? Quais serão os impactos tecnológicos e econômicos da expansão chinesa da rede 5G no mundo? Qual será o nível de penetração da tecnologia cibernética estrangeira na China? E como operam os objetivos de ciberdefesa dos demais países com respeito à China?

## REFERÊNCIAS

Béraud-Sudreau, Lucie. 2019. "China's 2019: Defence White Paper: The Long Road to Transparency in Defence Spending". *Military Balance Blog*. https://www.iiss.org/blogs/military-balance/2019/08/china-white-paper-defence-spending--transparency.

Birdwell, M. Bodine, and Robert Mills. 2011. "War fighting in cyberspace: evolving force presentation and command and control". *Air & Space Power Journal*: 26–36.

Blasko, Dennis J. 2006. *The Chinese Army Today*. Londres: Routledge.

Brasil. Ministério da Defesa. 2010. *Minuta de nota de coordenação doutrinária relativa ao I Seminário de Defesa Cibernética do Ministério da Defesa*. Brasília.

Brasil. Ministério da Defesa. 2015. *Glossário das Forças Armadas*. bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf.

Bull, Hedley. 2002. *The Anarchical Society : a Study of Order in World Politics*. New York: Columbia University Press.

Chang, Amy. 2014. *Warring States: China's Cybersecurity Strategy*. The Center for New American Security. www.cnas.org/publications/reports/warring-state-chinas-cybersecurity-strategy.

China. Ministry of National Defense of the People's Republic of China. 2013. *White Paper: The Diversified Employment of China's Armed Forces*. eng.mod.gov.cn/Database/WhitePapers/.

Clarke, R. A. 2012. *Cyber War: the next threat to national security and what to do about it*. New York: HarperCollins Publishers.

CNNIC. 2018. *The 41st statistical report on internet development in China*. www.cac.gov.cn/.

CPC. 2006. *2006–2020 National Informatization Development Strategy*. www.gov.cn/gongbao/content/2006/content_315999.htm.

Daricili, Ali Burak, and Barış Özdal. 2017. "The Analysis on the Instruments Forming the Cyber Security capacity of Russian Federation". *Bilig*, no. 83: 121–46.

Daricili, A. B., and Barış Özdal. 2018. "Analysis of the cyber security strategies of people's Republic of China". *Güvenlik Stratejileri Dergisi* 14, no. 28: 1–35. dergipark.org.tr/tr/download/article-file/594354. doi.org/10.17752/guvenlikstrtj.495748.

DeNardis, L. 2014. *The global war for internet governance*. New Haven: Yale University Press.

Document 27: Opinions for Strengthening Information Security Assurance Work. 2003. (《国家 信息化领导小组关于加强信息安全保障工作的 意见》, *guojia xinxihua lingdao xiaozu guanyu jiaqiang xinxi anquan baozhang gongzuo de yijian*).

Dornelles Jr., A. C. 2014. "A modernização militar da China e a distribuição de poder no Leste Asiático". *Contexto Internacional* 36 no. 1: 145–70.

Hathaway, M. et al. 2015. "Índice de pre-paración cibernética 2.0. Un plan para la preparación cibernética: una línea de base y un índice" *Potomac Institute for Policy Studies*. www.belfercenter.org/sites/default/files/files/publication/cyber-readiness-2.0-spanish-v2.pdf.

Herold, D. K. 2011. "An inter-nation-al Internet: China's contribution to global Internet governance?". *Symposium "Decade in Internet Time"*.

Hong, Yu, and G. Thomas Goodnight. 2019. "How to think about cyber sovereignty: the case of China". *Chinese Journal of Communication.*

Ibragimova, Galiya. 2017. "PRC Strategy in the field of internet management and ensuring the information security". *Security Index* 170: 1–19.

Jr., Ng. 2020. "China Broadens Cyber Options". *Asian Military Review Magazine.* asianmilitaryreview.com/2020/01/china-broadens-cyber-options/.

King, G., J. Pan, and M. E. Roberts. 2013. "How censorship in China allows government criticism but silences collective expression". *American Political Science Review* 107, no. 2: 326–43.

Kremer, J. 2014. "Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace", *Information & Communications Technology Law 23*, no. 3: 220–37.

Lanzetta, J. G. 2023. *Ciberespaço e o sistema internacional: uma análise da segurança cibernética do estado.* Trabalho de Conclusão — Curso de Bacharelado em Ciência Política. Santana do Livramento: Unipampa.

Lewis, J. A., and K. Timlin. 2011. *Cybersecurity and cyberwarfare: Preliminary assessment of national doctrine and organization.* Unidir.

Libicki, Martin C. 2012. *Crisis and Escalation in Cyberspace.* Santa Monica, CA: RAND Corporation. ISBN 978-0-8330-7678-6.

Liles, S., J. E. Dietz, M. Rogers, and D. Larson. 2012. "Applying traditional military principles to cyber warfare" in *4th International Conference on Cyber Conflict* 1-12.

Lira-Brito, R. V. 2020. *Defesa e Segurança Cibernéticas: crimes cibernéticos e políticas públicas no Brasil.* Trabalho de Conclusão de Curso — Bacharelado em Ciência Política. Recife: UFPE.

Lira-Brito, R. V. 2022. *Segurança Cibernética Comparada: o Brasil e as Américas.* Dissertação — Mestrado em Ciência Política. Recife: UFPE.

Liy, Macarena. 2017. "La polémica ley de ciberseguridad entra en vigor en China". *El País.* elpais.com/internacional/2017/05/31/actualidad/1496241283_691973.html.

Mackinnon, R. 2011. "China's 'networked authoritarianism'". *Journal of Democracy* 22, no. 2: 32–46.

Morgenthau, Hans J. 2003. *A política entre as nações: a luta pelo poder e pela paz*. Brasília: Editora UnB.

Negro, Gianluigi. 2019. "A history of Chinese global Internet governance and its relations with ITU and ICANN" *Chinese Journal of Communication*.

No, Nurkulov. 2017. "New Cyber Strategy of China and the Alterations in the Field" *Journal of Political Science & Public Affairs*.

Nye Jr, Joseph S. 2009. "Smart Power" *Novas Perspectivas Quarterly* 26, no. 2.

Nye Jr, Joseph S. 2011 *The Future of Power*. New York: Public Affairs.

Office of the Secretary of Defense. 2019. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*. Office of the Secretary of Defense.

Peron, Alcides E. dos R. 2016. "Guerra virtual e eliminação da fricção? O uso da cibernética em operações de contrainsurgência pelos EUA". In *Relações Internacionais Cibernéticas (CiberRI): oportunidades e desafios para os Estudos Estratégicos e de Segurança Internacional*, edited by Marcos A. Guedes de Oliveira, Ricardo B. Gama Neto, and Gills Vilar Lopes. Recife: Editora da UFPE (Defesa & muros virtuais, 3).

Portela, L. S. (2015) *Movimentos centrais e subjacentes no espaço cibernético do século XXI*. Dissertação (Mestrado em Ciências Militares), ECEME, Rio de Janeiro.

Rauchfleisch, A.; Schäfer, M. S. (2015) "Multiple public spheres of Weibo: A typology of forms and potentials of online public spheres in China" *Information, Communication & Society* 18, no. 2, 139–55.

Sátyro, N. G. D., and R. W. D'Albuquerque. 2020. "O que é um Estudo de Caso e quais as suas potencialidades". *Sociedade e Cultura* 23.

Shaohui, Tian (Ed.). 2017. "International Strategy of Cooperation on Cyberspace". *Xinhuanet*(Mar.).www.xinhuanet.com//english/china/2017-03/01/c_136094371.htm

Shen, Hong. 2017. "Across the Great (Fire) Wall: China and the global Internet".

Schreiber, C. 2019 "El futuro de China y Rusia como aliados en el ciberespacio". *Análisis GESI 2*, no. 1.

Teixeira Júnior, A., W. M.; G. Vilar-Lopes, and M. T. D. Freitas. 2017. "As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica". *Carta Internacional* 12, no. 3: 30–53.

Toso, Bruna (2016) "Poder Cibernético: Perspectivas para o Brasil". *I Seminário de Estudos Estratégicos*: 462–7.

UIT. 2009. *Guía de ciberseguridad para los países en desarrollo.* www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2007-PDF-S.pdf.

Unga. United Nations General Assembly. 2023. *Transforming Our World: The 2030 Agenda for Sustainable Development.* sdgs.un.org/2030agenda.

Ventre, D. 2011. "Ciberguerra". *XIX Curso Internacional de Defensa.* Seguridad global y potências emergentes em um mundo multipolar. Academia General Militar. Espanha: Universidad Zaragoza

Vilar-Lopes, G. 2017. Relações Internacionais cibernéticas (CiberRI): o impacto dos Estudos Estratégicos sobre o ciberespaço nas Relações Internacionais. *Congreso Latinoamericano de Ciência Política* v. 9.

Wasserman, H. 2018. "Power, meaning and geopolitics: Ethics as an entry point for global communication studies" *Journal of Communication* 68, no. 2: 441–51.

CIBERDEFESA E *SOFTWARE POWER*: UMA ANÁLISE EXPLORATÓRIA DA CHINA


## RESUMO

Como o *software power* ajuda a compreender a ciberdefesa e a projeção de poder na China? Os avanços tecnológicos e da Internet acrescentaram, nas Relações Internacionais, um novo espaço de disputas e de análise, o Espaço Cibernético, no qual os Estados passaram a traçar estratégias de defesa e expansão de poder que parecem se diferenciar daquelas mais tradicionais, que envolvem a coerção pela força (*hard power*) ou pelo convencimento (*soft power*). Há ainda uma terceira forma, que se expressa através de programas, sistemas, aplicativos e informações naquelas estruturas físicas e virtuais que compõem o Espaço Cibernético, o *Software Power*. Nesse sentido, o objetivo geral deste trabalho é compreender se esta forma de poder é utilizada nos moldes tradicionais de proliferação, ou seja, como uma ferramenta para manifestar os interesses estatais e atingir seus fins soberanos. Para tanto, utilizamos metodologia qualitativa, através de uma análise exploratória de documentos sobre o caso chinês, consistindo a estrutura em um estudo de caso. Dentre os resultados, observa-se que não há uma estratégia clara da política externa chinesa para impor ou convencer outros países sobre estes programas, aplicativos, sistemas e informações oriundos da China. Por outro lado, são identificados interesses, preocupações e questões internas para a defesa chinesa e sua blindagem às influências externas no Espaço Cibernético.


**Palavras-chave:** Ciberdefesa; Espaço cibernético; China; Projeção de poder; *Software Power*.


## ABSTRACT

How does software power help to understand cyber-defense and power projection in China? Advances in technology and the Internet have added to International Relations a new space for disputes and analysis, Cyberspace, in which States have begun to devise strategies for defense and expansion of power that seem to differ from the more traditional ones, which involve coercion through force (hard power) or persuasion (soft power). There is also a third form, which is expressed through programs, systems, applications and information in those physical and virtual structures that make up Cyberspace, Software Power. In this sense, the general objective of this work is to understand whether this form of power is used in the traditional way of proliferation, that is, as a tool to manifest state interests and achieve its sovereign ends. To this end, we used a qualitative methodology, through an exploratory analysis of documents on the Chinese case, with the structure consisting of a case study. The results show that there is no clear strategy in Chinese foreign policy to impose or convince other countries of these programs, applications, systems and information from China. On the other hand, internal interests, concerns and issues are identified for Chinese defense and its shielding from external influences in Cyberspace.


**Keywords:** Cyberdefense; Cyberspace; China; Power Projection; Software Power.

**Recebido em 23/12/2022. Aceito para publicação em 14/06/2024.**

NOTAS

1. Texto original: "*[...] a set of resources that relate to the creation, control, and communication of electronic and computer-based information – infrastructure, networks, softwares, human skills. This includes not only the Internet of networked computers, but also Intranets, cellular technologies, and space-based communications*".
2. State Informatization Leading Group (China), Document 27: Opinions for Strengthening Information Security Assurance Work (《国家 信息化领导小组关于加强信息安全保障工作的 意见》, *guojia xinxihua lingdao xiaozu guanyu jiaqiang xinxi anquan baozhang gongzuo de yijian*) (2003).
3. CPC Central Committee and State Council,2006–2020 nian guojia xinxihua fazhan zhanlüe (2006–2020 National Informatization Development Strategy), www.gov.cn/gongbao/content/2006/content_315999.htm].
4. Academy of Military Science Strategic Research Department, The Science of Military Strategy, (Beijing: Military Science Publishing House, 2013); Information Oce of the State Council, "White Paper: The Diversified Employment of China's Armed Forces," April 2013. Disponível em: [http://eng.mod.gov.cn/Database/WhitePapers/].
5. Este conceito foi originalmente criado por Mao Zedong, chamado "defesa ativa", que se baseia na premissa de atacar somente depois que o inimigo atacar, mas empregará ofensivas operações em todos os níveis da guerra e em todos os estágios do conflito.
6. A Organização de Cooperação de Xangai (SCO) foi fundada em 15 de junho de 2001, com o objetivo de fortalecer a confiança e a boa vizinhança entre seus membros, promovendo a cooperação em política, comércio, pesquisa, intercâmbio e desenvolvimento tecnológico e cultural, educação, transporte, energia, turismo e segurança, entre outros. Promove também respeito, confiança, benefício e igualdade mútua (Schreiber 2019).
7. De acordo com a *Cyberspace Administration of China* (CAC), o objeto desta lei é "salvaguardar a soberania no Espaço Cibernético, a segurança nacional e o interesse público, além dos direitos e interesses dos cidadãos".
8. Relatório da Comissão dos Assuntos Externos e pareceres da Comissão do Comércio Internacional e da Comissão do Ambiente, da Saúde Pública e da Segurança Alimentar (A8-0252/2018), inc. 'P' in Proposta de Resolução do Parlamento Europeu, sobre o estado das relações entre UE e a China (2017/2274 (INI)).
9. *El país*, 2017. "La polémica ley de ciberseguridad entra en vigor en China". elpais.com/internacional/2017/05/31/actualidad/1496241283_691973.html [24 jan. 2022]
10. Para efeitos de defesa terrestre, o ELP conta com vários ramos ou armas (*bingzhong*) e unidades de apoio, tais como: infantaria, artilharia, unidades de defesa aérea; unidade de engenheira; defesa química; comunicações, móveis e fixas; guerra eletrônica, incluindo unidades de contramedida ele-

trônica (ECM); logística, incluindo suprimentos (*quartermaster*), petróleo, óleo e lubrificantes (POL), unidades médicas e de transporte, incluindo unidades de caminhões e navios; unidades de armamento, responsáveis pela manutenção, reparo e armazenamento de munições (Blasko, 2019: 20).

11. "Rise in China's defense budget to outpace economic growth target", *Reuters*, 4 mar. 2019. https://uk.reuters.com/article/us-china-parliament-defence-idUSKCN1QM03Y [23 jan. 2022]
12. *Asian Military Review Magazine*. "China Broadens Cyber Options", 2020. https://asianmilitaryreview.com/2020/01/china-broadens-cyber-options/ [24 jan. 2022]
13. Sobre este aspecto, acusações, por parte do governo dos EUA de um suposto uso da rede 5G para espionagem, pela empresa chinesa Huawei, ilustram esta disputa em diferentes partes do mundo.
14. "China planejar aliviar regras sobre as gigantes da tecnologia para estimular economia", *Valor Econômico*, 30 abr. 2022. https://valor.globo.com/mundo/noticia/2022/04/30/china-planejar-aliviar-regras-sobre-as-gigantes-da-tecnologia-para-estimular-economia.ghtml [21 maio 2022]