liinc EM REVISTA

ARTIGO/ARTICLE

Cibersegurança como soberania nacional? Perspectivas do Brasil e da China[1]

Cybersecurity as National Sovereignty? Perspectives from Brazil and China

Mayara Araujo
Universidade Federal Fluminese (UFF). Programa de Pós-Graduação em Comunicação (PPGCOM). Niterói, RJ, Brasil.

Aline Mendes
Universidade Federal Fluminese (UFF). Programa de Pós-Graduação em Comunicação (PPGCOM). Niterói, RJ, Brasil.

Correspondência para/Correspondence to
Mayara Araujo - soareslpa@yahoo.com.br

Periódico / Journal
ISSN 1808-3536
@liinc-emrevista
https://revista.ibict.br/liinc/index

Editores / Editors
Marco Schneider
Gustavo Saldanha
Fábio Gouveia

Fluxo editorial / Editorial process
Editores do Artigo / Article Editors
Fábio Guedes Gomes - José Medeiros
Marco Schneider - Chen Lan

Cronologia / Timeline
Recebido / Received: 03/04/2025
Aprovado / Approved: 21/05/2025
Publicado / Published: 27/06/2025

Como citar / How to cite: ARAUJO, Mayara; MENDES, David. Cibersegurança como soberania nacional? Perspectivas do Brasil e da China. *In*: *Liinc em Revista*, v. 21, n. 01, e7548. Disponível em: https://revista.ibict.br/liinc/article/view/7548. Acesso em: 30 jun. 2025.

[1] A Liinc em Revista teve o apoio da **FAPERJ** para a publicação deste artigo.

RESUMO: Este artigo examina a cibersegurança como fator estratégico de soberania nacional, comparando as perspectivas do Brasil e da China. Discutem-se a ascensão das "guerras de informação" e a relevância crescente do ambiente cibernético nos conflitos contemporâneos, evidenciando como a segurança digital se tornou tema central em documentos de defesa. Metodologicamente, adota-se uma abordagem descritivo-comparativa, com base na análise dos Livros Brancos de Defesa da China (2023) e do Brasil (2020). Enquanto a China lida com questões relacionadas ao ciberespaço por meio de um sólido arcabouço jurídico, alinhado ao fortalecimento do Estado e ao desenvolvimento nacional, o Brasil trata a segurança cibernética como um domínio do Exército, focando ameaças a infraestruturas digitais nacionais, sem sustentar maiores conexões com o desenvolvimento nacional.

Palavras-chave: cibersegurança soberania, Internet, Brasil, China.

ABSTRACT: This article examines cybersecurity as a strategic factor of national sovereignty, comparing the perspectives of Brazil and China. It discusses the rise of "information wars" and the growing relevance of the cyber environment in contemporary conflicts, highlighting how digital security has become a central theme in defense documents. Methodologically, the study adopts a descriptive-comparative approach based on the analysis of China's Defense White Paper (2023) and Brazil's Defense White Paper (2020). While China addresses cyberspace-related issues through a robust legal framework aligned with state strengthening and national development, Brazil treats cybersecurity as a military domain, primarily managed by the Army and focused on threats to national digital infrastructures, without deeper connections to national development.

Keywords: cybersecurity, Sovereignty, Internet, Brazil, China.

INTRODUÇÃO

"A revolução da informação e as inovações organizacionais associadas estão transformando os conflitos, assim como as estruturas, doutrinas e estratégias militares necessárias" (Arquilla; Ronfeldt, 1993, p. 141). Esse processo levou à ascensão do setor cibernético como um recurso decisivo na conjuntura internacional. Já na década de 1990, argumentava-se que as "guerras de informação" e as "guerras cibernéticas" seriam centrais no século XXI, conferindo vantagem àqueles que dominassem as redes nos conflitos transnacionais (Arquilla; Ronfeldt, 1993). Assim, não surpreende que a cibersegurança seja um dos temas centrais nos livros brancos de defesa dos países, sendo tratada como uma questão crítica de segurança nacional.

Com a automação de cada vez mais atividades comerciais e a expansão do uso da inteligência artificial (IA), cresce também o volume de informações confidenciais armazenadas em computadores. Isso torna a segurança dos sistemas ainda mais essencial, especialmente em um cenário em que aplicativos e plataformas operam de forma distribuída e dependem da internet, uma rede naturalmente vulnerável (Kemmerer, 2003). A internet é vista como uma rede insegura, pois pode ser alvo de ataques de diferentes locais, tornando difícil proteger completamente os dados e recursos armazenados por empresas, organizações e Estados. As redes computacionais sustentam diversas atividades, e qualquer interferência externa pode afetar ou até paralisar empresas, órgãos governamentais e organizações. Exemplo disso foi o ataque *hacker* ao Sistema Eletrônico de Informações brasileiro em julho de 2024, que afetou funções essenciais de nove ministérios (Estadão, 2024). Com a crescente dependência das redes computacionais, a segurança cibernética deixou de ser apenas uma questão técnica e passou a ser um elemento central da segurança nacional (Kemmerer, 2003), especialmente por seu papel na manutenção da soberania dos Estados e no controle de suas fronteiras digitais.

A cibersegurança é um desafio complexo, que exige planejamento e desenvolvimento contínuo, não podendo ser garantida com medidas improvisadas ou soluções pontuais (Kemmerer, 2003). Proteger redes e sistemas depende de estratégias bem-estruturadas, que envolvem tanto tecnologia quanto políticas de segurança e capacitação constante. Os países estabelecem diferentes diretrizes em seus livros de defesa nacionais para proteger esse campo estratégico, essencial à estabilidade e à soberania das nações. Diante disso, analisamos como Brasil e China entendem a segurança cibernética e quais medidas adotam para enfrentar ameaças digitais e garantir sua soberania. Ao contrastar essas duas abordagens, o artigo contribui para o debate sobre cibersegurança, destacando diferentes estratégias e caminhos possíveis. Observamos que, na China, a segurança cibernética está ancorada em um extenso arcabouço jurídico, pensado para reforçar tanto o poder do Estado quanto o desenvolvimento do país. No Brasil, por outro lado, o tema fica restrito ao Exército, com foco na proteção de infraestruturas digitais, mas sem conexão mais clara com um projeto de soberania nacional.

Adotamos um desenho qualitativo, comparando Brasil e China com inspiração na análise documental (Bowen, 2009) e com apoio da pesquisa bibliográfica. Os Livros Brancos de Defesa do Brasil (2020) e da China (2023) foram localizados em repositórios governamentais e selecionados por serem as versões mais recentes e por constituírem documentos estratégicos de referência. Seguiu-se o ciclo proposto por Bowen (2009): localização, seleção, avaliação da autenticidade e síntese. Trabalhamos

com dados provenientes dos documentos, extraindo deles informações que nos ajudam a compreender as perspectivas brasileira e chinesa em torno da articulação entre segurança cibernética e soberania nacional. Com isso, visamos a responder aos seguintes questionamentos: Como o Brasil e a China delineiam suas perspectivas a respeito da segurança cibernética e dialogam com suas maneiras de entender a soberania nacional? Quais medidas são adotadas para alcançar essa finalidade? O artigo está estruturado da seguinte forma: a primeira seção discorre sobre os conceitos de soberania e cibersegurança; já a segunda e a terceira exploram a noção de cibersegurança conforme exposta nos livros brancos. Começamos pela China e, em seguida, o Brasil.

SOBERANIA E CIBERSEGURANÇA

A expansão e a consequente popularização do uso da internet no globo tiveram impactos significativos em nossa forma de estar no mundo, gerando afetações em termos de nossas formas de comunicação e interação social, mas também impactando a produção e a disseminação de cultura, o ambiente público no qual as políticas são estruturadas e a transformação do ambiente econômico. O ecossistema digital alcançou uma escala global, ultrapassando as fronteiras territoriais (Nunes, 2012) e afetando as dinâmicas geopolíticas contemporâneas. Para além de possíveis benefícios, os países também se apropriam dessa infraestrutura digital para propagar seus objetivos externos. No caso do uso de plataformas digitais, esse movimento tem sido compreendido à luz do que teóricos do campo das relações internacionais chamam de "diplomacia digital", que enfatiza o uso dessa tecnologia como ferramentas para a busca de suas aspirações na política externa (Adesina, 2017). A China é um bom exemplo de como os países têm se apropriado das possibilidades da emergência das plataformas digitais para se posicionarem publicamente. No perfil oficial da Embaixada da China no Brasil no Instagram, sua equipe de comunicação não apenas divulga informações sobre as relações sino-brasileiras, mas também aproveita a ferramenta para ampliar o alcance de seus posicionamentos internacionais.

Por outro lado, o enfraquecimento das fronteiras no espaço digital também impõe desafios críticos à manutenção da soberania dos Estados. O conceito clássico de soberania está relacionado à territorialidade e envolve a centralização do poder em uma instância decisória final, livre de intervenções externas, com autoridade para manter a ordem pública (Barros, 2009). O controle das fronteiras e a gestão autônoma das dinâmicas internas sem interferência externa figuram entre os pilares centrais da soberania nacional. No entanto, a soberania, que antes era percebida como um dos conceitos mais efetivos para compreender o sistema internacional, hoje é contestada por uma visão que defende a improbabilidade de o Estado soberano manter-se como o principal *locus* de autoridade política e comunidade no futuro, pois a soberania é desafiada por novas configurações de autoridade e comunidades que transcendem a divisão entre as esferas doméstica e internacional (Bartelson, 2006).

Entre os fatores que têm posto em xeque a manutenção da soberania dos países estão a interligação frequente dos mercados financeiros, que dificultam as capacidades estatais de controlar as políticas fiscais e monetárias, a crescente influência de empresas transnacionais que desafiam as leis internas dos Estados (Barros, 2009) e o ambiente digital, que também pode se chocar com as jurisdições nacionais (Carvalho, 2018) e implicar ameaças diretas à soberania dos Estados, como no caso de

ataques cibernéticos e, mais recentemente, de empreitadas de plataformas digitais estrangeiras que desafiam as leis locais, como foi o bloqueio do Twitter/X no Brasil (Steil, 2024).

Aqui, nossa ênfase recai sobre o primeiro caso mencionado: os ataques cibernéticos. Essas investidas deram origem a novas formas de conflito, como as guerras cibernéticas, nas quais operações militares são conduzidas com base em princípios de informação. O objetivo consiste em interromper ou destruir os sistemas de comunicação e informação do adversário, garantindo vantagem na balança de informação e conhecimento. Além de manipular o fluxo informacional do oponente, os ataques às redes podem fornecer dados estratégicos essenciais, ampliando a compreensão sobre vulnerabilidades, posicionamentos e recursos do inimigo — um fator decisivo na condução de conflitos (Arquilla; Ronfeldt, 1993). Outra modalidade de conflito é o que os autores chamam de "infoguerra", ou seja, uma modalidade de combate que procura alterar, enfraquecer ou manipular o conhecimento que uma população tem sobre si mesma e o mundo. Nisso, direciona-se à opinião pública e/ou às elites, utilizando estratégias a partir do uso de propaganda, campanhas psicológicas e subversão cultural e política. As infoguerras também podem envolver o controle da mídia, o acionamento de desinformação, a infiltração em redes e bancos de dados, além do estímulo a movimentos dissidentes por meio das infraestruturas digitais (Arquilla; Ronfeldt, 1993). Embora os autores tenham sido pioneiros na atribuição do conceito, cabe destacar que, na década de 1990, outros pesquisadores discorreram sobre noções em torno das guerras de informação, como Waltz (1998), Schwartau (1995) e Libicki (1995).

As "guerras de quarta geração" emergiram após o fim da Guerra Fria (1947-1991), refletindo a crescente influência asiática e a urbanização dos conflitos. Nesse contexto, a população passou a sentir mais diretamente seus impactos, como choques culturais e ações terroristas (Rodrigues, 2020). Essa nova fase da guerra manteve elementos das gerações anteriores, como grupos reduzidos, logística descentralizada e foco na desestabilização interna do inimigo, mas se diferenciou pelo uso ampliado de tecnologias de alta precisão, armas mais sofisticadas e maior proteção dos combatentes. Além disso, a evolução dos meios de comunicação tornou os conflitos mais difusos, enquanto as guerras cibernéticas, psicológicas e informacionais redefinem as estratégias de dominação e controle, expandindo o alcance dos embates e desafiando as noções tradicionais de guerra (Rodrigues, 2020).

A guerra híbrida, por fim, atua como tentativa de desestabilização de algum governo, que muitas vezes se limita à agitação no âmbito da sociedade civil, mas que pode acabar se desdobrando em uma segunda fase, na qual há emprego da violência (Korybko, 2018). As plataformas algorítmicas são uma atmosfera especialmente favorável à guerra híbrida, cujas manifestações têm sido cada vez mais potencializadas por elas (Castro, 2020). Embora também se valham de táticas da infoguerra, seu objetivo é impactar as dimensões física e psicológica do conflito, e pode ser conduzida tanto por Estados quanto por atores não estatais (Hoffman, 2007). As ameaças cibernéticas fazem parte do escopo dessa modalidade de ataque, interferindo diretamente na segurança nacional e desestabilizando governos locais ou nacionais (Rodrigues, 2020).

Ao abordar dinâmicas ligadas à defesa nacional, como guerras cibernéticas, guerras híbridas e infoguerras, os ataques cibernéticos costumam ser associados a outros países ou a grupos paramilitares de grande expressão, como organizações terroristas e o crime organizado. No entanto,

Liinc em Revista, Rio de Janeiro, v. 21, n. 01, e7548, jun. 2025.
https://doi.org/10.18617/liinc.v21i1.7548

aspectos como espionagem,[2] manipulação[3] e desinformação,[4] presentes nessas modalidades de guerra, também podem ser conduzidos por empresas privadas de tecnologia sem ligação explícita com atores estatais ou grupos criminosos. O escândalo da Cambridge Analytica exemplifica essa questão, pois a empresa coletou ilegalmente dados pessoais de usuários do Facebook e os utilizou para interferir em processos eleitorais. Essa ação privada manipulou tendências políticas, comprometendo a democracia (Fornasier; Beck, 2020) e a integridade da informação dos usuários. Assim, plataformas digitais transnacionais, mesmo sem vínculo direto com Estados, podem representar um risco à defesa e à soberania dos países, ainda que suas ações nem sempre se encaixem nas definições tradicionais de guerra cibernética.

É com base em suas próprias noções a respeito da segurança nacional que as diretrizes sobre a cibersegurança são estabelecidas. A forma como as nações pensam a cibersegurança, portanto, serve à finalidade de fortalecer suas estratégias de defesa, proteger infraestruturas críticas e consolidar o exercício de sua soberania nacional de maneira abrangente. Afinal, hoje faz pouco sentido separar a esfera física da digital. Dito isso, utilizamos a seguir o caso da China e do Brasil para discorrer a respeito das convergências e divergências sobre o tema por parte das duas nações, com base em seus mais recentes livros brancos publicados.

CIBERSEGURANÇA NA CHINA

Embora a China tenha conexão à internet desde a década de 1980, é a partir de 1994 que essa ferramenta se tornou de amplo alcance. De lá para cá, o país asiático conta com mais de 1 bilhão de usuários conectados (CNNIC, 2022) e tem se dedicado à governança cibernética baseada na lei, garantindo que o desenvolvimento da internet chinesa ocorra dentro dos limites legais (China, 2023). A quantidade de normas referentes ao controle da internet vem aumentando expressivamente nas últimas décadas. Em um levantamento de dados sobre a governança da internet realizado por Yang e Mueller (2014), estima-se que 57% das políticas estavam relacionadas à regulamentação de conteúdo, enquanto 41% dos documentos concentravam-se na noção de cibersegurança. Os autores destacam que, desde 2006, as autoridades chinesas passaram a enfatizar mais essas duas temáticas e que em diversos documentos elas pareciam estreitamente interligadas.

Questões relativas à produção e à disseminação de conteúdos falsos em plataformas digitais têm sido alvo de preocupação de diversos países (Allcoot; Gentzkow, 2017; Delmazo; Valente, 2018). Na China, esse tópico entra em debate em campanhas como, por exemplo, a Operação Rede Limpa, que visa a lidar com problemas relativos à desinformação e ao *bullying* na internet. *Sites* e plataformas que disseminam informações que violam leis e regulamentos têm recebido advertências administrativas, ordens de retificação e notificações, além de punições, como multas e suspensões temporárias na

[2] A espionagem cibernética refere-se à finalidade de testar a configuração e os sistemas de defesa de um computador específico ou obter acesso a informações confidenciais (Fonseca, 2021).

[3] Tratamos de manipulação com base no aporte de Ienca (2023), que define manipulação no cenário digital como qualquer influência exercida por meio do uso de tecnologia digital intencionalmente projetada para contornar a razão e produzir uma assimetria de resultados entre o processador de dados (ou um terceiro que se beneficie dele) e o titular dos dados.

[4] A desinformação, nesse contexto, pode ser entendida como informação enganosa, cuja capacidade de causar erro é prevista, ainda que não haja necessariamente a intenção direta de enganar. Isso inclui desde conteúdos falsos até informações verdadeiras apresentadas de forma a induzir o público ao erro, o que torna a desinformação um instrumento potente, mesmo quando disseminada como efeito colateral (Fallis, 2009).

publicação de novos conteúdos. Mas não somente. De acordo com o Livro Branco de 2023, *sites* e plataformas têm sido instados a assumir responsabilidade principal, gerenciando as informações divulgadas por seus usuários de acordo com a lei e seus próprios termos de uso (China, 2023). Pelo fato de a China ter construído um ecossistema de plataformas próprias, o país consegue se defender, em alguma medida, de táticas de guerra híbrida por parte de atores estrangeiros (Korybko, 2018). Nessa direção, sua consistente estrutura jurídica em torno das plataformas digitais se apresenta como instrumento de preservação contra interferências externas nesse âmbito.

Em uma publicação mais recente, destaca-se que, de 1994 a 2017, contabilizam-se mais de 350 documentos jurídicos dedicados ao gerenciamento da rede (Miao; Jiang; Pang, 2021), entre os quais se destacam a Lei de Cibersegurança da China, de 2017, e a Lei de Segurança de Dados, de 2021. Trata-se de documentos que vêm, inclusive, sendo alvo de discussões acadêmicas (Liu *et al.*, 2022; Qi; Shao; Zheng, 2018). Esse arcabouço legislativo faz parte da estratégia reguladora conduzida pela China, o *Golden Shield Project*, que ficou conhecida no Ocidente como a "Grande *Firewall* Chinesa", na qual o governo chinês estabelece o gerenciamento da internet por meio de instrumentos como a fiscalização e a retenção do conteúdo e de legislações que servem de apoio a essa regulação.

São mais de 70 agências reguladoras que têm participação na produção de políticas para a internet na China, sendo algumas mais expressivas do que as outras: de 1996 a 2017, o Ministério da Indústria e da Tecnologia da Informação, uma das principais entidades reguladoras do país, publicou mais de 90 documentos legais na área; o Ministério Público da Segurança, outra instituição de destaque, publicou 56 (Miao; Jiang; Pang, 2021). Em relação à cibersegurança, destaca-se que ela está sob supervisão de diversos ministérios, como o Ministério da Segurança Pública, o Ministério da Indústria e Tecnologia da Informação, a Administração Nacional para a Proteção de Segredos de Estado e o Ministério da Cultura (Yang; Mueller, 2014). Atualmente, conta-se também com o envolvimento da Administração do Ciberespaço da China.

As agências ocupam o terceiro nível dentro da estrutura regulatória chinesa, junto às comissões e aos departamentos correlacionados. No segundo nível, encontram-se a Suprema Corte, a Procuradoria Nacional e o Conselho de Estado. Nesse contexto, o Conselho de Estado tem papel fundamental ao supervisionar o trabalho das agências em conjunto com a Administração do Ciberespaço e ao produzir documentos legais. No topo dessa estrutura, acima dos dois níveis mencionados, está a Assembleia Popular Nacional, que atua em parceria com o Comitê Permanente, responsável, por exemplo, pela formulação e regulamentação da Lei de Cibersegurança da China e que se configura como a principal autoridade na aprovação de leis relacionadas à internet (Vieira, 2023). De acordo com as diretrizes do Partido Comunista Chinês, a legislação chinesa abrange um amplo conjunto de normas, que inclui leis, interpretações judiciais, regulações administrativas, decretos locais, decretos autônomos, decretos especiais e demais regras, todas estruturadas sob o arcabouço constitucional da China (Miao; Jiang; Pang, 2021).

A noção chinesa de soberania digital se encontra diretamente interligada com a noção de soberania como fonte de poder do Estado e tem a cibersegurança como um de seus pilares centrais. A soberania digital chinesa vai na contramão de perspectivas que entendem a internet como um espaço que promove uma liberdade irrestrita e abre espaço, portanto, para uma noção que vê a regulação digital como caminho para proteger e ampliar o poder estatal, seja na esfera política ou na econômica (Vieira,

2023). Isso pode ser ilustrado a partir da criação do órgão de Administração do Ciberespaço da China, em 2014, que responde diretamente ao presidente do país e que tem o posto mais elevado entre as agências que regulam o tema (Miao; Jiang; Pang, 2021). Concomitantemente, a regulação da internet passou a ser vista como parte da estratégia nacional a partir do *slogan* "sem cibersegurança, sem segurança nacional" (Creemers; Trilo; Webster, 2018). Segundo o documento publicado em 2017:

> Cibersegurança [网络安全, também "segurança de rede"] refere-se à adoção de medidas necessárias para prevenir ataques cibernéticos, intrusões, interferências, destruição e uso ilegal, bem como acidentes inesperados, a fim de manter as redes em um estado de operação estável e confiável, além de garantir que os dados da rede sejam completos, confidenciais e utilizáveis. (Lei de Cibersegurança da China, 2017, tradução nossa)

Já em 2023, a China publicou o Livro Branco de Defesa *China's law-based cyberspace governance in the new era*, no qual as autoridades chinesas propõem apresentar os avanços na gestão do ciberespaço, ao mesmo tempo que compartilham a experiência chinesa. Nele, destaca-se a cibersegurança como elemento central da segurança nacional, estruturando um arcabouço legal e institucional para proteger redes, sistemas de informação, dados e infraestrutura crítica contra ameaças cibernéticas. A legislação chinesa estabelece três eixos principais: a definição de regras para garantir a segurança das operações de rede, produtos e serviços *online*; a proteção da infraestrutura crítica de informação, essencial para a soberania digital e o funcionamento socioeconômico do país; e a gestão da segurança de dados, com mecanismos para classificação, monitoramento de riscos e transparência dos dados governamentais (China, 2023). Observa-se, portanto, uma evolução na visão chinesa a respeito da cibersegurança, uma vez que, nesse documento, passa-se a inseri-la em uma estratégia mais ampla de segurança nacional e como importante pilar para o desenvolvimento nacional.

A China entende que a governança de um país deve ser estabelecida a partir de leis bem-estruturadas, e com a internet não seria diferente. Para isso, "a China tem aprimorado seu sistema jurídico para a governança do ciberespaço por meio de uma legislação concebida de maneira criteriosa, democrática e em conformidade com a lei" (China, 2023, p. 7, tradução nossa). Nesse sentido, a legislação do ciberespaço chinesa contou com três fases: de 1994 a 1999, quando a China promoveu a conexão à internet, levando ao aumento no número de usuários e dispositivos. A legislação estava concentrada na segurança da infraestrutura de rede, principalmente na proteção dos sistemas computacionais. Já o segundo momento, entre os anos 2000 e 2011, foi marcado pelo aumento do uso de computadores pessoais como a principal plataforma de acesso à internet. Em um período de popularização de serviços baseados na *web*, a legislação enfatizou a regulamentação dos serviços e a gestão do conteúdo *online*. A terceira fase, iniciada em 2012, é dominada pela internet móvel. A legislação agora se orienta para uma governança abrangente do ciberespaço, abordando áreas como serviços de informação *online*, desenvolvimento de tecnologias da informação e segurança cibernética (China, 2023).

Ao longo dos anos, a China consolidou um arcabouço legislativo para a governança do ciberespaço com mais de 140 leis que estruturam essa regulação. Ancorado na Constituição, esse sistema se desdobra em leis, regulamentos administrativos, normas departamentais e regras regionais, combinando a legislação tradicional com marcos específicos para a gestão de conteúdo *online*, segurança cibernética, proteção de dados e desenvolvimento tecnológico. Esse conjunto normativo

estabelece bases institucionais para reforçar a atuação da China no ambiente digital, conforme o Quadro 1 ilustra.

Quadro 1. Legislação cibernética na China

Tipo	Exemplos
Leis	• Lei do Comércio Eletrônico • Lei da Assinatura Eletrônica • Lei de Segurança Cibernética • Lei de Segurança de Dados • Lei de Proteção de Informações Pessoais • Lei de Combate à Fraude em Telecomunicações e *Online*
Regulamentos administrativos	• Regulamentos sobre a Segurança e a Proteção dos Sistemas de Informação Computadorizados • Regulamentos sobre a Proteção de *Software* de Computador • Medidas Administrativas para Serviços de Informação na Internet • Regulamentos de Telecomunicações • Regulamentos sobre a Administração do Investimento Estrangeiro em Empresas de Telecomunicações na China • Regulamentos sobre a Proteção do Direito de Comunicação por Meio de Redes de Informação • Regulamentos sobre a Segurança e a Proteção da Infraestrutura Crítica de Informação
Regras departamentais	• Regulamentos sobre a Proteção das Informações Pessoais de Crianças na Internet • Regulamentos sobre Nomes de Domínio da Internet na China • Medidas para a Supervisão e Administração de Transações *Online* • Disposições sobre a Administração de Serviços de Notícias e Informações na Internet • Regulamentos sobre a Governança de Informação e Conteúdo *Online* • Regulamentos sobre a Gestão de Recomendações Algorítmicas para Serviços de Informação na Internet
Regulamentos locais	• Lei de Promoção da Economia Digital da Província de Guangdong • Lei de Promoção da Economia Digital da Província de Zhejiang • Regulamentos da Província de Hebei sobre o Desenvolvimento da Tecnologia da Informação • Regulamentos da Província de Guizhou sobre Compartilhamento de Dados Governamentais • Regulamentos Municipais de Xangai sobre Dados
Regras administrativas locais	• Medidas da Província de Guangdong sobre a Gestão de Dados Públicos • Medidas da Província de Anhui sobre a Gestão de Dados e Recursos para Assuntos Governamentais • Medidas da Província de Jiangxi sobre a Proteção da Segurança dos Sistemas de Informação Computadorizados • Medidas Provisórias da Cidade de Hangzhou sobre a Administração de Transações *Online*
Número total	Mais de 140

Fonte: China, 2023.

Liinc em Revista, Rio de Janeiro, v. 21, n. 01, e7548, jun. 2025.
https://doi.org/10.18617/liinc.v21i1.7548

Para além das perspectivas focadas em sua própria realidade, o Livro Branco de Defesa (2023) também destaca que as experiências de outros países também serviram como fonte de aprendizado para que a China pudesse desenvolver seu próprio modelo de governança do ciberespaço. Alinhada a seus interesses nacionais de construção de um país socialista moderno, a China reafirma seu compromisso em uma governança da internet ancorada em leis que foram sendo moldadas a partir da identificação de necessidades por parte do Estado e concebe que a proteção do ciberespaço está diretamente vinculada à sua própria noção de soberania nacional. Não somente, esse documento defende que esse arcabouço institucional é o pano de fundo que sustenta o estímulo à inovação, que, consequentemente, gera crescimento econômico para o país. É com a convergência entre o desenvolvimento tecnológico e o ordenamento do espaço digital que se delineia um material constitutivo para o desenvolvimento econômico chinês. Do ponto de vista da China, não parece haver maiores distinções entre o desenvolvimento seguro do ciberespaço e seu próprio desenvolvimento nacional.

CIBERSEGURANÇA NO BRASIL

Desde 1996, no documento Política Nacional de Defesa (PND), que estabelece os objetivos e as diretrizes para a defesa nacional, já se discutia o desenvolvimento tecnológico como um recurso fundamental para a autonomia estratégica da segurança nacional, especialmente no âmbito das Forças Armadas. No início dos anos 2000, a cibersegurança foi incorporada à dinâmica de defesa nacional brasileira, quando as atividades de segurança da informação passaram a ser tratadas pelo recém-criado Gabinete de Segurança Institucional da Presidência da República (GSI/PR). Anos mais tarde, em 2006, o GSI/PR criou o Departamento de Segurança da Informação e Comunicações (DSIC), responsável por planejar e coordenar a implementação das atividades de segurança da informação e comunicações na Administração Pública Federal (Brasil, 2014b). As atribuições do DSIC foram posteriormente ampliadas, passando a abarcar o planejamento e a coordenação das ações de segurança cibernética e de segurança da informação e comunicações na Administração Pública Federal.

A consolidação da cibersegurança como domínio de defesa nacional só ocorreu em 2012, quando o Centro de Defesa Cibernética, vinculado ao Comando do Exército, passou a coordenar e a integrar as ações de defesa cibernética no Ministério da Defesa. Nesse mesmo ano, foi aprovada a Política Cibernética de Defesa e, com a publicação do Livro Branco de 2012, definiram-se diretrizes para proteger o setor cibernético (Brasil, 2014a). Em seguida, a PND de 2013 elevou a tecnologia a um campo estratégico, capaz de reforçar a eficiência administrativa e militar do país — embora também gerasse novas vulnerabilidades, como interferências remotas. Assim, a cibersegurança firmou-se como campo essencial para a defesa nacional, e a PND estabeleceu metas claras para esse fim, tais como

> […] aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação ou permitam seu pronto restabelecimento. (Brasil, 2013, p. 9)

Liinc em Revista, Rio de Janeiro, v. 21, n. 01, e7548, jun. 2025.
https://doi.org/10.18617/liinc.v21i1.7548

E "a redução da dependência tecnológica e à superação das restrições unilaterais de acesso a tecnologias sensíveis" (Brasil, 2013, p. 8).

Esse breve recorte histórico ilustra que as diretivas para lidar com os ataques cibernéticos no país foram sendo estruturadas somente ao longo do século XXI, a despeito de o país estar conectado à internet desde 1988 (Alencar, 2011). Nesse sentido, ataques cibernéticos passaram a ser vistos como questão de defesa nacional por parte das autoridades brasileiras (Brasil, 2020), e foi estabelecido que o setor cibernético deveria ser tratado como tão estratégico para a proteção nacional quanto os setores espacial e nuclear. No entanto, enquanto questões relacionadas ao setor nuclear ficaram sob a coordenação da Marinha e ao setor espacial com a Força Aérea, o debate em torno do setor cibernético ficou nas mãos do Exército. Isso se alinha à perspectiva sustentada por Arquilla e Ronfeldt (1993), que previam a centralidade do setor cibernético na defesa dos países durante o século XXI.

Essa divisão categórica entre as forças de segurança foi estabelecida por meio de diretrizes do Ministério da Defesa ainda em 2009. O Exército tem cinco comandos de aplicação específicos, dos quais dois estão voltados para a área cibernética: o Comando de Comunicações e Guerra Eletrônica do Exército (CComGEx) e o Comando de Defesa Cibernética (ComDCiber) (Brasil, 2020). Cada um deles detém atribuições específicas e coordena setores subordinados, conforme o Quadro 2.

Quadro 2. A cibersegurança no Exército Brasileiro

Comandos de segurança cibernética do Exército	**Definição**	**Atribuições**	**Subordinados**
Comando de Comunicações e Guerra Eletrônica do Exército (CComGEx)	O CComGEx surgiu da fusão da antiga Diretoria de Material de Comunicações Eletrônica e Informática (DMCEI) com o Centro de Instrução de Guerra Eletrônica (Cige) (Brasil, 20--a)	O CComGEx foca sua atuação na logística de comunicações, eletrônica e informática por meio do Centro Logístico, além da capacitação em comunicações, guerra eletrônica e cibernética pela Escola de Comunicações e Centro de Instrução de Guerra Eletrônica. Também coordena e planeja o subsistema de detecção e apoio à decisão do Sistema Integrado de Monitoramento de Fronteiras (Sisfron) (Brasil, 20--a)	Companhia de Comando e Controle (Cia C2); Cige; base administrativa; Escola de Comunicações (Escom)
Comando de Defesa Cibernética (ComDCiber)	Comando operacional conjunto, integrante da estrutura regimental do Exército e subordinado ao Departamento de Ciência e Tecnologia (DCT) (Brasil, 2024b)	"Planejar, orientar, supervisionar e controlar as atividades operacional, de inteligência, doutrinária, de ciência e tecnologia, bem como de capacitação no Setor Cibernético de Defesa" (Brasil, 2020, p. 47)	Centro de Defesa Cibernética (CDCiber) e Escola Nacional de Defesa Cibernética (ENaDCiber)

Fonte: elaborado pelo autor (2025).

Liinc em Revista, Rio de Janeiro, v. 21, n. 01, e7548, jun. 2025.
https://doi.org/10.18617/liinc.v21i1.7548

O CComGEx concentra suas atividades centrais em procedimentos logísticos, nos quais se incube das "etapas de aquisição, armazenamento, controle, distribuição e utilização dos equipamentos de comunicações pelas diversas Organizações Militares do Exército" (Paysan, 2019, p. 16). Ou seja, as diversas funções logísticas relacionadas às comunicações táticas e tecnologias da informação operacional estão sob responsabilidade do CComGEx (Paysan, 2019). Esse órgão também lida com o 1º Batalhão de Guerra Eletrônica, voltado para três atividades: medidas de ataque eletrônico (MAE), medidas de apoio à guerra eletrônica (Mage) e medidas de proteção eletrônica (MPE) (Okamura, 2018). Enquanto os dois últimos grupos são voltados para a obtenção de informações inimigas e para a segurança das transmissões próprias, o ramo das MAE consiste em ações mais ativas, destinadas a dificultar ou a impedir o uso do espectro eletromagnético por parte dos oponentes (Okamura, 2018). Já o 1º Batalhão de Guerra Eletrônica, especializado em guerra eletrônica, cibernética e comunicações (Brasil, 2024a), detém os equipamentos para realizar o bloqueio de transmissores de radiofrequência e de drones, além de atuar em apoio aos grandes eventos que podem ocorrer no país (Okamura, 2018). O CComGEx também supervisiona a Escola de Comunicações (Escom), a Companhia de Comando e Controle (Cia C2) e o Centro de Instrução de Guerra Eletrônica (Cige). A Escom oferece cursos de comunicação, tecnologia e cibersegurança (Brasil, [20--b]); a Cia C2 mantém sistemas de comunicação e comando para operações militares; e o Cige capacita recursos humanos em guerra eletrônica e cibernética, fortalecendo a Força Terrestre (Brasil, [20--b]).

O ComDCiber integra a estrutura de cibersegurança do Exército, com militares da Marinha e da Força Aérea, operando como um comando conjunto (Brasil, 2022). Sua missão é garantir que as Forças Armadas brasileiras usem o espaço cibernético com eficácia, ao mesmo tempo que impeçam ou dificultem que ele seja explorado contra os interesses da Defesa Nacional (Brasil, 2017). Para isso, realiza exercícios e simulações para avaliar a proteção do país contra ataques cibernéticos (Brasil, 2024c). Também assessora o ministro da Defesa na gestão do Sistema Militar de Defesa Cibernética, assegurando a interoperabilidade e a segurança dos sistemas (Brasil, 2023).

Entre as unidades subordinadas ao ComDCiber estão o Centro de Defesa Cibernética (CDCiber) e a Escola Nacional de Defesa Cibernética (ENaDCiber). O CDCiber é encarregado de coordenar e integrar todas as atividades de defesa cibernética dentro do Ministério da Defesa (Brasil, 2017). Suas atribuições incluem a organização do centro, o tratamento da documentação referente à segurança cibernética, a gestão de pessoal e a coordenação de projetos, como a Rede Nacional da Segurança da Informação e Criptografia (Renasic) (Brasil, 2014a). A Renasic, por sua vez, foi criada para ampliar as competências brasileiras em segurança da informação e criptografia. Ela funciona por meio de laboratórios distribuídos pelo país que atuam de forma colaborativa em rede, envolvendo centenas de pesquisadores universitários em projetos de cibersegurança (Barretto, 2020).

O Livro Branco de Defesa (Brasil, 2020) destaca que a proteção do espaço cibernético envolve capacitação, inteligência, pesquisa, doutrina, preparo operacional, gestão de pessoal, proteção de ativos e atuação em rede. No entanto, não define "segurança cibernética", concentrando-se na descrição de ameaças e medidas adotadas. Sob a coordenação do Exército, o documento enfatiza avanços na formação de especialistas e no desenvolvimento de soluções tecnológicas. As funções dos comandos e órgãos subordinados refletem essa abordagem, priorizando capacitação, gestão de pessoal, atuação em rede e preparo operacional. Apesar do escopo amplo, há limitações, especialmente na proteção da soberania nacional. O setor é tratado como domínio do Exército, com

Liinc em Revista, Rio de Janeiro, v. 21, n. 01, e7548, jun. 2025.
https://doi.org/10.18617/liinc.v21i1.7548

cooperação restrita à Marinha, à Força Aérea e a acadêmicos por meio da Renasic, enquanto a participação de atores não militares é reduzida, inclusive em cursos de capacitação. Isso pode limitar estratégias mais amplas contra ameaças cibernéticas. Além disso, as ações do Exército na área são pouco divulgadas. Nem a plataforma do Exército Brasileiro nem o CComGEx disponibilizam informações sobre inovação tecnológica ou projetos em andamento. Embora os objetivos sejam divulgados, falta transparência sobre as iniciativas em curso, e não há uma plataforma centralizada com esses dados.

Essa falta de transparência se mantém intacta mesmo em situações de ataques cibernéticos a entidades governamentais brasileiras. Desde 2024, por exemplo, plataformas de organizações governamentais brasileiras têm sido alvo de ataques de um *hacker* (Grossmann, 2025). No entanto, os comandos responsáveis por garantir a segurança cibernética no país nunca divulgaram medidas para identificar o atacante, nem mesmo divulgam quais medidas estão sendo adotadas para reforçar a proteção dessas plataformas. Na ocasião dos ataques direcionados ao Superior Tribunal de Justiça (2024 e 2025) e ao Conselho Nacional de Justiça (2025), não foi sequer mencionada a participação dos comandos do Exército como instrumentos de defesa. Esses eventos levantam questões a respeito da capacidade nacional de lidar com ataques mais complexos e estruturados, como guerras cibernéticas promovidas por outros países.

A segurança nacional é entendida como

> […] a preservação da soberania e da integridade territorial, a realização dos interesses nacionais, a despeito de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais. (Brasil, 2020, p. 193)

Os ataques cibernéticos, ao criarem pressões e ameaças à segurança do país e de seus cidadãos, evidenciam a vulnerabilidade brasileira nesse campo, o que representa séria ameaça à segurança nacional. Além disso, a limitação do escopo de segurança cibernética abordado no Livro Branco de 2020, restrito às estruturas estratégicas do país, representa um desafio para a soberania nacional, uma vez que parece desconsiderar a sociedade civil. A soberania é definida como

> […] a manutenção da intangibilidade da Nação, assegurada a capacidade de autodeterminação e de convivência com as demais nações em termos de igualdade de direitos, não aceitando qualquer forma de intervenção em seus assuntos internos, nem participação em atos dessa natureza em relação a outras nações. (Brasil, 2020, p. 193)

Tanto essa definição de soberania quanto a concepção brasileira sobre as ameaças cibernéticas no Brasil ignoram dinâmicas mais complexas, uma vez que também podem abranger a intervenção de atores não estatais. Questões relativas à infoguerra (Arquilla; Ronfeldt, 1993) e às guerras híbridas (Hoffman, 2007) não exigem coordenação estatal para causar impactos estratégicos. Além disso, ameaças como desinformação, roubo de dados e vigilância sem consentimento representam riscos não apenas à soberania dos Estados, mas também ao exercício pleno da cidadania. Casos como o escândalo Facebook-Cambridge Analytica e as revelações de espionagem da Agência Nacional de Segurança dos Estados Unidos (NSA, do inglês National Security Agency) contra a então presidenta Dilma Rousseff (Bridi; Greenwald, 2013) expuseram diretamente cidadãos brasileiros a essas

Liinc em Revista, Rio de Janeiro, v. 21, n. 01, e7548, jun. 2025.
https://doi.org/10.18617/liinc.v21i1.7548

vulnerabilidades, mas o Livro Branco (Brasil, 2020) parece negligenciar tais fatores, mesmo tratando-os como prioritários para a defesa nacional. Episódios como os vivenciados por Dilma Rousseff não apenas expõem as fragilidades técnicas, mas também reforçam, no âmbito da soberania nacional, a urgência de consolidar estruturas de ciberdefesa capazes de proteger tanto os altos escalões do governo quanto a privacidade dos cidadãos.

Ao centrar o conceito de soberania nacional em interferências estatais, o Ministério da Defesa adota uma visão limitada de cibersegurança, dando prioridade a conflitos cibernéticos e a ataques contra infraestruturas estratégicas. Embora o Livro Branco de 2020 reconheça que as investidas *online* podem ter diferentes origens, ele deixa de lado ameaças como o uso estratégico de desinformação e o roubo de dados. Nesse contexto, as medidas de segurança cibernética coordenadas pelo Exército mostram-se pouco abrangentes e ineficientes, pois não incluem a sociedade civil em seu escopo de proteção. Isso abre espaço para que atores não estatais, como *hackers* e empresas estrangeiras, comprometam tanto a soberania nacional quanto a proteção da população brasileira.

CONCLUSÕES

O artigo apresentou uma análise comparativa sobre como China e Brasil compreendem a cibersegurança, enfatizando seu papel estratégico na garantia da soberania nacional. Inicialmente, discutimos o conceito de soberania e sua conexão com a ascensão do ciberespaço, evidenciando-se o crescimento das "guerras de informação" e o uso da internet como recurso de poder e controle nas relações internacionais. Em seguida, exploramos o caso chinês, caracterizado por um sistema legal e institucional, que engloba diversos dispositivos legislativos, todos voltados para regulamentar plataformas, segurança de dados e conteúdo *online*. Já no caso brasileiro, destacam-se a atribuição do setor cibernético ao Exército, a criação de comandos específicos e a relativa limitação na abordagem mais ampla da segurança digital. Os rumos e as escolhas estruturais de cada país refletem dinâmicas próprias de inserção na agenda global de cibersegurança.

Observamos que ambos os países reconhecem a importância de proteger infraestruturas críticas e de se preparar para possíveis conflitos híbridos. No entanto, enquanto a China vem apostando na criação de um arcabouço jurídico consistente para reforçar o papel do Estado e impulsionar sua estratégia de crescimento nacional, o Brasil lida com uma estrutura mais fragmentada, na qual a proteção cibernética está sob responsabilidade principal do Exército e, muitas vezes, dissociada de um plano de desenvolvimento econômico e nacional. Entendemos que a China adotou uma abordagem estatal e intervencionista de governança do ciberespaço, sustentada por um extenso aparato de restrições sancionado pelas leis chinesas (Dong, 2012), o que se torna viável dentro de seu próprio modelo político vigente. O Brasil, por sua vez, está inserido em um contexto constitucional que impõe limites claros à atuação estatal no ambiente digital (Tomasevicius Filho, 2016). Reconhecer essas diferenças implica compreender as limitações envolvidas em qualquer tentativa de transposição direta de modelos entre os dois países. Não se trata, aqui, de sugerir que um modelo deva servir de referência para o outro de forma acrítica. Pelo contrário: o exercício comparativo proposto busca evidenciar as divergências entre as abordagens e extrair delas elementos que contribuam para o fortalecimento de uma estratégia de soberania digital brasileira condizente com seu próprio contexto.

Liinc em Revista, Rio de Janeiro, v. 21, n. 01, e7548, jun. 2025.
https://doi.org/10.18617/liinc.v21i1.7548

A forma como cada país consolida sua estratégia cibernética molda não apenas a proteção de redes e sistemas, mas também a própria capacidade de manter a autonomia e a autodeterminação no ambiente digital. A promoção de uma visão integrada, que una regulação, desenvolvimento tecnológico e inovação, e a participação de diferentes atores são essenciais para o fortalecimento da soberania nacional, principalmente diante de um contexto cada vez mais conectado e sujeito a interferências externas.

Liinc em Revista, Rio de Janeiro, v. 21, n. 01, e7548, jun. 2025.
https://doi.org/10.18617/liinc.v21i1.7548

REFERÊNCIAS

ADESINA, O. Foreign policy in an era of digital diplomacy. **Cogent Social Sciences**, [*s. l.*], v. 3, n. 1, p. 1-13, 2017. Disponível em: https://www.tandfonline.com/doi/full/10.1080/23311886.2017.1297175. Acesso em: 6 mar. 2025.

ALENCAR, M. Evolução da internet. **Revista de Tecnologia da Informação e Comunicação**, Campina Grande, v. 1, n. 1, p. 6-10, 2011. Disponível em: https://www.academia.edu/72231416/Evolu%C3%A7%C3%A3o_da_Internet. Acesso em: 6 mar. 2025.

ALLCOOT, H.; GENTZKOW, M. Social media and fake news in the 2016 election. **Journal of Economic Perspectives**, [*s. l.*], v. 31, n. 2, p. 211-236, 2017. DOI: https://doi.org/10.1257/jep.31.2.211. Disponível em: https://www.aeaweb.org/articles?id=10.1257/jep.31.2.211 . Acesso em: 6 mar. 2025.

ARQUILLA, J.; RONFELDT, D. Cyberwar is coming!. **Comparative Strategy**, [*s. l.*], v. 12, n. 2, p. 141-165, 1993. DOI: https://doi.org/10.1080/01495939308402915. Disponível: https://www.rand.org/pubs/reprints/RP223.html. Acesso em: 6 mar. 2025.

BARRETTO, A. Exército Brasileiro fortalece mais a sua defesa cibernética no país. **Revista Operacional**, 2020. Disponível em: https://www.revistaoperacional.com.br/exercito/exercito-brasileiro-fortalece-mais-a-sua-defesa-cibernetica-no-pais/. Acesso em: 5 mar. 2025.

BARROS, A. Soberania e República em Jean Bodin. **Discurso**: Revista do Departamento de Filosofia da USP, São Paulo, n. 39, p. 59-84, 2009. DOI: 10.11606/issn.2318-8863.discurso.2009.68264. Disponível em: https://www.academia.edu/79958172/Soberania_e_Rep%C3%BAblica_em_Jean_Bodin. Acesso em: 6 mar. 2025.

BARTELSON, J. **The concept of sovereignty revisited**. Oxford, Inglaterra: Oxford University Press, 2006.

BOWEN, G. Document analysis as a qualitative research method. **Qualitative Research Journal**, [*s. l.*], v. 9, n. 2, p. 27-40, 2009. DOI: https://doi.org/10.3316/QRJ0902027. Disponível em: https://www.ufsm.br/app/uploads/sites/479/2023/06/Bowen-2009.pdf. Acesso em: 16 maio 2025.

BRASIL. Departamento de Ciência e Tecnologia do CComGEx. **Companhia de Comando e Controle CIA C2**. Brasília, DF: Exército Brasileiro, 2022. Disponível em: https://www.ccomgex.eb.mil.br/dpdg/arquivos/Cia%20C2.pdf. Acesso em: 5 mar. 2025.

BRASIL. Departamento de Ciência e Tecnologia do CComGEx. **Histórico**. Brasília, DF: Exército Brasileiro, [20--a]. Disponível em: https://www.ccomgex.eb.mil.br/index.php/en/historico. Acesso em: 3 mar. 2025.

BRASIL. Departamento de Ciência e Tecnologia do CComGEx. **Visita operacional do comandante de operações terrestres ao CMD de comunicações e guerra eletrônica do Exército**. Brasília, DF: Exército Brasileiro, 2024a. Disponível em: https://www.eb.mil.br/web/noticias/w/visita-operacional-do-cmt-de-operacoes-terrestres-ao-comando-de-comunicacoes-e-guerra-eletronica-do-exercito. Acesso em: 3 mar. 2025.

BRASIL. Escola de Comunicações. **Cursos realizados na EsCom**. Brasília, DF: Exército Brasileiro, [20--b]. Disponível em: http://www.escom.eb.mil.br/cursos. Acesso em: 5 mar. 2025.

BRASIL. Exército Brasileiro. **Liberdade de ação no espaço cibernético**. EPEX, 2024b. Disponível em: https://encurtador.com.br/cBaeg. Acesso em: 3 mar. 2025.

BRASIL. Marinha do Brasil. Marinha participa da maior simulação de defesa cibernética do Hemisfério Sul. **Agência Gov**, 15 out. 2024c. Disponível em: https://agenciagov.ebc.com.br/noticias/202410/marinha-participa-da-maior-simulacao-de-defesa-cibernetica-do-hemisferio-sul. Acesso em: 5 mar. 2025.

BRASIL. Ministério da Defesa. Centro de Defesa Cibernética. **CDCIBER**: perspectivas em face da espionagem eletrônica. Brasília, DF: Ministério da Defesa, 2014a. Disponível em: https://encurtador.com.br/Fnk23. Acesso em: 5 mar. 2025.

BRASIL. Ministério da Defesa. **Comando Conjunto na Defesa Cibernética**. Brasília, DF: Ministério da Defesa, 26 abr. 2017. Disponível em: https://www.gov.br/defesa/pt-br/centrais-de-conteudo/noticias/ultimas-noticias/comando-conjunto-na-defesa-cibernetica. Acesso em: 5 mar. 2025.

BRASIL. Ministério da Defesa. **Doutrina militar de defesa cibernética**. Brasília, DF: Ministério da Defesa, 2014b. Disponível em: https://encurtador.com.br/coo9w. Acesso em: 24 fev. 2025.

BRASIL. Ministério da Defesa. **Doutrina militar de defesa cibernética**. Brasília, DF: Ministério da Defesa, 25 out. 2023. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31M07DoutrinaMilitardeDefesaCiberntica2Edio2023.pdf. Acesso em: 5 mar. 2025.

BRASIL. Ministério da Defesa. **Livro branco de defesa nacional 2020**. Brasília, DF: Ministério da Defesa, 2020. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/estado_e_defesa/livro_branco/Versaodolivroemportugues2020.pdf. Acesso em: 2 fev. 2025.

BRASIL. Ministério da Defesa. **Política nacional de defesa**. Brasília, DF: Ministério da Defesa, 25 set. 2013. Disponível em: https://bibliotecadigital.economia.gov.br/handle/123456789/461. Acesso em: 17 maio 2025.

BRIDI, S.; GREENWALD, G. Documentos revelam esquema de agência dos EUA para espionar Dilma. **G1**, 1 set. 2013. Disponível em: https://g1.globo.com/fantastico/noticia/2013/09/documentos-revelam-esquema-de-agencia-dos-eua-para-espionar-dilma-rousseff.html. Acesso em: 18 maio 2025.

CARVALHO, L. Soberania digital: legitimidade e eficácia da aplicação da lei na internet. **Revista Brasileira de Direito**, [*s. l.*], v. 14, n. 2, p. 213-235, 2018. Disponível em: https://seer.atitus.edu.br/index.php/revistadedireito/article/view/2183. Acesso em: 6 mar. 2025.

CASTRO, J. Máquinas de guerra híbrida em plataformas algorítmicas. **E-Compós**, [*s. l.*], v. 23, n. 1, p. 1-29, 2020. Disponível em: https://www.e-compos.org.br/e-compos/article/view/1929. Acesso em: 6 mar. 2025.

CHINA. **Governança do ciberespaço baseada em leis na China na nova era**. Conselho de Estado da República Popular da China, 16 mar. 2023. Disponível em:

https://english.www.gov.cn/archive/whitepaper/202303/16/content_WS6489542ec6d0868f4e8dcd56.html. Acesso em: 11 fev. 2025.

CNNIC – China Internet Network Information Center. **48º relatório de estatísticas internet na China**. 2021. Disponível em: https://www.cnnic.com.cn/IDR/ReportDownloads/202111/P020211119394556095096.pdf. Acesso em: 1 mar. 2025.

CNNIC – China Internet Network Information Center. **50º relatório de estatísticas internet na China**. 2022. Disponível em: https://www.cnnic.com.cn/IDR/ReportDownloads/202212/P020230829504457839260.pdf. Acesso em: 1 mar. 2025.

CREEMERS, R.; TRIOLO, P.; WEBSTER, G. **Translation**: Xi Jinping's April 20 speech at the National Cybersecurity and Informatization Work Conference. [*S. l.*]: Stanford University, 29 jun. 2018. Disponível em: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/. Acesso em: 6 mar. 2025.

DELMAZO, C.; VALENTE, J. Fake news nas redes sociais online: propagação e reações à desinformação em busca de cliques. **Media & Jornalismo**, [*s. l.*], v. 18, n. 32, p. 155-169, 2018. Disponível em: https://impactum-journals.uc.pt/mj/article/view/2183-5462_32_11. Acesso em: 6 mar. 2025.

DONG, F. Controlling the internet in China: the real story. **Convergence**, [*s. l.*], v. 18, n. 4, p. 403-425, 2012. Disponível em: https://journals.sagepub.com/doi/10.1177/1354856512439500. Acesso em: 16 maio 2025.

ESTADÃO. Ataque hacker: o que se sabe sobre ação que derrubou sistemas de ministérios. **CNN Brasil**, 25 jul. 2024. Disponível em: https://www.cnnbrasil.com.br/politica/o-que-se-sabe-sobre-o-ataque-hacker-que-derrubou-sistemas-de-ministerios/. Acesso em: 24 fev. 2025.

FALLIS, D. A conceptual analysis of disinformation. *In*: ICONFERENCE, 2009, Chapel Hill, NC. **Proceedings** [...]. [*S. l.: s. n.*], 2009. Disponível em: https://www.ideals.illinois.edu/items/15210. Acesso em: 6 mar. 2025.

FONSECA, L. A cibersegurança sob o prisma das relações internacionais. **Relações Exteriores**, 20 out. 2021. Disponível em: https://relacoesexteriores.com.br/ciberseguranca-relacoes-internacionais/. Acesso em: 20 maio 2025.

FORNASIER, M.; BECK, C. Cambridge Analytica: escândalo, legado e possíveis futuros para a democracia. **Revista Direito em Debate**, [*s. l.*], v. 29, n. 53, p. 182-195, 2020. Disponível em: https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/10033. Acesso em: 6 mar. 2025.

GROSSMANN, L. STJ: ataque cibernético não atingiu sistemas. **Convergência Digital**, 5 mar. 2025. Disponível em: https://convergenciadigital.com.br/seguranca/stj-ataque-cibernetico-nao-atingiu-sistemas/. Acesso em: 5 mar. 2025.

HOFFMAN, F. **Conflict in the 21st century**: the rise of hybrid wars. Arlington, Estados Unidos: Potomac Institute for Policy Studies, 2007.

IENCA, M. On artificial intelligence and manipulation. **Topoi**, [*s. l.*], v. 42, n. 3, p. 833-842, 2023. Disponível em: https://link.springer.com/article/10.1007/s11245-023-09940-3. Acesso em: 20 maio 2025.

KEMMERER, R. Cybersecurity. *In*: INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING, 25., 2003, Portland. **Anais** [...]. [*S. l.*]: IEEE Computer Society, 2003. Disponível em: https://dl.acm.org/doi/abs/10.5555/776816.776918. Acesso em: 24 fev. 2025.

KORYBKO, A. **Guerras híbridas**: das revoluções coloridas aos golpes. São Paulo: Expressão Popular, 2018.

LIBICKI, Martin**. What is information warfare?** Center for Advanced Concepts and Technology, Institute for National Strategic Studies, 1995.

LIU, Y.; HUANG, L.; YAN, W.; WANG, X.; ZHANG, R. Privacy in AI and the IoT: the privacy concerns of smart speaker users and the Personal Information Protection Law in China. **Telecommunications Policy**, [*s. l.*], v. 46, n. 7, 2022. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0308596122000362?via%3Dihub. Acesso em: 6 mar. 2025.

MIAO, W.; JIANG, M.; PANG, Y. Historicizing internet regulation in China: meta-analysis of Chinese internet policies (1994-2017). **International Journal of Communication**, [*s. l.*], v. 15, p. 2003-2026, 2021. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4852245. Acesso em: 6 mar. 2025.

NUNES, P. F. A definição de uma estratégia nacional de cibersegurança. **Nação e Defesa**, [*s. l.*], v. 5, n. 133, p. 113-127, 2012. Disponível em: https://revistas.rcaap.pt/nacao/article/view/38475. Acesso em: 6 mar. 2025.

OKAMURA, A. **O emprego de medidas de ataque eletrônico no apoio da guerra eletrônica aos grandes eventos**. 2018. Trabalho de Conclusão de Curso (Especialização em Ciências Militares), Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, Rio de Janeiro, 2018.

PAYSAN, W. **A gestão do material classe VII – equipamentos de comunicações táticas e de tecnologia da informação operacional – no Exército Brasileiro**. 2019. Trabalho de Conclusão de Curso (Especialização em Ciências Militares), Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, Rio de Janeiro, 2019.

QI, A.; SHAO, G.; ZHENG, W. Assessing China's Cybersecurity Law. **Computer Law & Security Review**, [*s. l.*], v. 34, n. 6, p. 1342-1354, 2018. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364918303157?via%3Dihub. Acesso em: 6 mar. 2025.

RODRIGUES, F. Guerra híbrida: por uma discussão conceitual. **Centro de Estudos Estratégicos do Exército**: Análise Estratégica, [*s. l.*], v. 18, n. 4, p. 23-36, 2020. Disponível em: https://ebrevistas.eb.mil.br/CEEExAE/article/view/7012/6051. Acesso em: 6 mar. 2025.

SCHWARTAU, W. **Information warfare**: chaos on the electronic superhighway. New York: Thunder's Mouth Press, 1995. 432 p.

STEIL, J. X fora do ar? Entenda medida de Alexandre de Moraes contra Elon Musk. **Valor**, 2024. Disponível em: https://valor.globo.com/politica/noticia/2024/08/29/elon-musk-descumpriu-a-lei-brasileira-entenda-por-que-o-x-pode-ficar-fora-do-ar.ghtml. Acesso em: 6 mar. 2024.

TOMASEVICIUS FILHO, E. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, [*s. l.*], v. 30, n. 86, p. 269-285, jan. 2016. Disponível em: https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/?lang=pt. Acesso em: 16 maio 2025.

VIEIRA, L. **Soberania, direitos humanos e cibersegurança**: a perspectiva chinesa para a regulação da internet. 2023. Dissertação (Mestrado em Relações Internacionais), Universidade Federal da Bahia, Salvador, 2023.

WALTZ, E. **Information warfare**. London: Artech House, 1998. 416 p.

YANG, F.; MUELLER, M. L. Internet governance in China: a content analysis. **Chinese Journal of Communication**, [China], v. 7, n. 1, p. 446-465, 2014. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/17544750.2014.936954. Acesso em: 6 mar. 2025.