



## Abordagem chinesa para a cibersegurança do Brics: conceitos, práticas e perspectivas<sup>1</sup>

China's Approach to BRICS Cybersecurity: Concepts, Practices and Prospect

**Fangfang Zhang** 

Beijing Foreign Studies University (BFSU), Department of Hispanic and Portuguese.  
Haidian District, Beijing, China.

**Junxuan Wu** 

Beijing Foreign Studies University (BFSU), Department of Hispanic and Portuguese.  
Haidian District, Beijing, China.

Correspondência para/Correspondence to  
Fangfang Zhang - [zhangfangfang@bfsu.edu.cn](mailto:zhangfangfang@bfsu.edu.cn)  
Junxuan Wu - [1029435923@qq.com](mailto:1029435923@qq.com)

### PERIÓDICO / JOURNAL

ISSN 1808-3536

 @liinc-emrevista

 <https://revista.ibict.br/liinc/index>

### FLUXO EDITORIAL / EDITORIAL PROCESS

Editores do Artigo / Article Editors

Fábio Guedes Gomes - José Medeiros

Marco Schneider - Chen Lan

### Editores / Editors

Marco Schneider

Gustavo Saldanha

Fábio Gouveia

### Cronologia / Timeline

Recebido / Received: 13/03/2025

Aprovado / Approved: 21/05/2025

Publicado / Published: 30/07/2025

Como citar / How to cite: ZHANG, Fangfang; WU, Juxuan. A infraestrutura humana da desinformação: um estudo de caso do trabalho heteromatizado no Brasil. In: *Liinc em Revista*, v. 21, n. 01, e7549. Disponível em: <https://revista.ibict.br/liinc/article/view/7549>. Acesso em: 30 jul. 2025.



Atribuição 4.0 Internacional  
Attribution 4.0 International

<sup>1</sup> Este artigo é um resultado parcial do projeto de pesquisa "Caminhos para o Aprimoramento das Competências Linguísticas nos Países BRICS e Mecanismos de Garantia Política no Contexto da Ascensão do 'Sul Global'" (nº do projeto YB145-137), aprovado em 2024 no âmbito do Plano de Pesquisa Científica do 14º Plano Quinquenal da Comissão Nacional de Língua e Escrita da China (projeto ministerial geral para jovens pesquisadores).

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

**RESUMO:** Embora a expansão acelerada da conectividade e o surgimento inovador de novas tecnologias de informação e comunicação tenham propiciado inúmeras oportunidades para indivíduos e empresas, é inegável que também trouxeram consigo uma série de desafios complexos. Nesse contexto, os países do Brics enfrentam ameaças comuns no campo da cibersegurança, tais como ataques cibernéticos, crimes cibernéticos e terrorismo cibernético, e precisam urgentemente encontrar soluções. A China, membro do Brics, tem sido proativa na formulação de estratégias para lidar com esses desafios. O estudo, por meio de revisão sistemática da literatura e análise de casos, visa a identificar leis e iniciativas chinesas de cibersegurança, fundamentais para o avanço da China na construção de uma sólida estrutura política para a cibersegurança, na ampliação da infraestrutura de comunicações digitais e na promoção do desenvolvimento do setor de cibersegurança, e a analisar oportunidades e desafios para a cooperação cibernética entre eles, propondo estratégias concretas. Espera-se apresentar padrões de políticas chinesas como referência, fornecendo a base para fortalecer a cooperação cibernética entre os países do Brics nas áreas da harmonização de políticas e regulamentações, da construção de uma infraestrutura global de informações interconectada e do estabelecimento de um eficaz mecanismo de comunicação.

**Palavras-chave:** China, cibersegurança, governança do ciberespaço, Brics.

**ABSTRACT:** While the accelerated expansion of connectivity and the innovative emergence of new information and communication technologies have provided countless opportunities for individuals and companies, it is undeniable that they have also brought with them a series of complex challenges. In this context, the BRICS countries face common threats in the field of cybersecurity, such as cyberattacks, cybercrime and cyber terrorism, and urgently need solutions. BRICS member China has been proactive in formulating strategies to deal with these challenges. This study, through a systematic review of the literature and case analysis, aims to identify the Chinese laws and initiatives which have been key to China's progress in building a solid cybersecurity policy framework, expanding digital communications infrastructure and promoting the development of the cybersecurity sector and to analyze the opportunities and challenges for cyber cooperation among the BRICS countries, and then propose specific strategies. It is expected that through this research, Chinese policy patterns as a reference can be introduced, providing a basis for strengthening BRICS countries' cyber cooperation in the areas of harmonizing policies and regulations, building an interconnected global information infrastructure and establishing an effective communication mechanism.

**Keywords:** China, cybersecurity, cyberspace governance, BRICS.

## INTRODUÇÃO

Atualmente, com o avanço da nova revolução científica e tecnológica e das transformações industriais, as tecnologias emergentes têm alterado profundamente o modo de produção e a vida humana. Embora essas novas tecnologias atendam às necessidades das pessoas por uma vida melhor, elas também representam desafios sem precedentes para a segurança nacional e a estabilidade social. A segurança da rede é uma componente crucial da segurança nacional. A construção de uma barreira sólida de cibersegurança nacional e a proteção eficaz da segurança do ciberespaço tornaram-se importantes tarefas estratégicas relacionadas ao desenvolvimento geral de cada país.

Os países do Brics enfrentam ameaças comuns à cibersegurança e precisam urgentemente encontrar soluções. Como membro do grupo, a China tem obtido notáveis conquistas na governança do ciberespaço, as quais são de grande importância para a governança cibernética global e a cooperação do Brics em cibersegurança. Este estudo tem como objetivo apresentar as práticas da China na área de cibersegurança, analisar a possibilidade de cooperação entre os países do Brics no domínio da cibersegurança e, com base nas experiências chinesas e nas ameaças comuns enfrentadas, identificar oportunidades e estratégias para fortalecer a cooperação cibernética entre os países do grupo.

O trabalho adotará uma abordagem multidisciplinar, combinando análises de políticas públicas e estudos de caso. A revisão sistemática da literatura será usada para identificar as principais políticas e práticas de cibersegurança da China e dos outros países do Brics. Análises de dados e casos de sucesso e fracasso serão usados para entender melhor os desafios e as oportunidades da cooperação cibernética entre os países do grupo.

Os resultados esperados incluem a identificação de políticas e práticas de cibersegurança da China que podem ser adaptadas para o contexto dos outros países do Brics, a análise das principais barreiras e oportunidades para a cooperação cibernética entre os países do grupo e o desenvolvimento de estratégias concretas para fortalecer essa cooperação. Esses resultados esperados contribuirão para a construção de um ciberespaço mais seguro e estável para todos os países do Brics.

## AMEAÇAS COMUNS À CIBERSEGURANÇA DO BRICS

Na era da informação, o avanço das novas tecnologias representa desafios sem precedentes para a cibersegurança. Nesse contexto, os membros do Brics enfrentam três ameaças comuns à cibersegurança.

A primeira ameaça é o ataque cibernético. Segundo Tsagourias (2012), “ataque cibernético” geralmente se refere a uma atividade cibernética realizada no ciberespaço, com o objetivo de desmontar, interromper, negar ou destruir informações armazenadas em um computador, ou de danificar o próprio computador. Essa ação afeta adversamente o computador ou a rede em questão e também coloca em risco as instalações do sistema ou o pessoal associado ao referido computador. Em razão das características do ciberespaço, os ataques cibernéticos são marcados por anonimato, furtividade e imediatismo (Li, 2023). Nos últimos anos, por causa da vulnerabilidade da infraestrutura

de informações, as infraestruturas críticas de informações, como finanças, eletricidade, transporte e sistemas de energia, têm sido os principais alvos de ataques cibernéticos (Gao, 2018).

A segunda ameaça é o crime cibernético. “Crime cibernético” é uma atividade criminosa, que pode ocorrer em qualquer localização geográfica, dada a natureza global da internet. Seu alvo é normalmente um computador, uma rede de computadores ou um dispositivo conectado à rede. A maior parte dos crimes é cometida por cibercriminosos ou *hackers*, com o objetivo de obter ganhos financeiros ilícitos (Silva, 2018). As economias emergentes têm altas taxas de crime cibernético. De acordo com a empresa McAfee, as maiores vítimas do crime cibernético são encontradas nas economias emergentes do Brics: Rússia, China e África do Sul, exatamente onde a conectividade é alta, mas a segurança e a conscientização sobre o crime cibernético são baixas (Gao, 2018).

A terceira ameaça é o terrorismo cibernético. “Terrorismo cibernético” se refere à utilização de técnicas por parte de terroristas visando a interromper ou a desativar as redes de informação computacionais. A internet se destaca entre essas redes por seu crescente fluxo de informações, importância estratégica, abrangência global e extensão geográfica (Barreto, 2007). O Brics está ameaçado pelo terrorismo cibernético. O Índice Global de Terrorismo (GTI, do inglês *Global Terrorism Index*) 2024, divulgado pelo Instituto para Economia e Paz (IEP), indicou que o índice de terrorismo da Índia, da Rússia, do Brasil, da China e da África do Sul está na 14<sup>a</sup>, 35<sup>a</sup>, 49<sup>a</sup>, 73<sup>a</sup> e 89<sup>a</sup> posições do mundo,<sup>2</sup> respectivamente. Isso demonstra que os países do Brics enfrentam ameaças terroristas em diferentes graus. A Índia é a mais afetada, seguida da Rússia, do Brasil e da China, enquanto a África do Sul enfrenta o menor nível de ameaças nesse domínio.

## CONCEITOS FORMULADOS PELO GOVERNO CHINÊS SOBRE A CIBERSEGURANÇA

As políticas de cibersegurança da China representam um elemento fundamental nas discussões globais e no contexto do Brics sobre a segurança cibernética no atual ambiente geopolítico. A China sempre atribui grande importância à governança da cibersegurança. O presidente chinês reiterou a necessidade de fortalecer a cooperação na governança da cibersegurança entre os países do Brics em várias oportunidades públicas. Prova disso é o fato de que a China formulou diversos conceitos no combate às ameaças cibernéticas, buscando contribuir para a construção de um espaço cibernético seguro e estável tanto para os países do Brics quanto para a comunidade internacional como um todo.

### Conceitos sobre ataque cibernético

No plano político, a atual administração chinesa promulgou várias leis e estratégias nacionais com o objetivo de fortalecer as capacidades de defesa cibernética da China. A Lei de Segurança Nacional da República Popular da China (2015) oferece um arcabouço abrangente para a segurança nacional e a segurança cibernética. A Estratégia Internacional da Cooperação no Ciberespaço (2016)<sup>3</sup> tem papel

<sup>2</sup> INSTITUTE FOR ECONOMICS & PEACE. **Global terrorism index 2024**. [S. l.: s. n.], 2024.

<sup>3</sup> Estratégia Internacional da Cooperação no Ciberespaço. **Xinhua**, 1 mar. 2017. Disponível em: [https://www.gov.cn/xinwen/2017-03/01/content\\_5172323.htm#1](https://www.gov.cn/xinwen/2017-03/01/content_5172323.htm#1)

de importância na governança cibernética internacional e na divulgação do apelo do presidente Xi Jinping para “estabelecer uma comunidade de futuro compartilhado no ciberespaço”. A Estratégia Militar da China (2015)<sup>4</sup> e a Defesa Nacional da China na Nova Era (2019)<sup>5</sup> constituem dois importantes livros brancos sobre estratégias de defesa chinesa e fornecem mais detalhes das estratégias militares cibernéticas da China. Especificamente, a Estratégia Militar da China aponta as deficiências do país em cibersegurança e a necessidade urgente de proteger as infraestruturas críticas. A Defesa Nacional da China na Nova Era deixa claro que o país está interessado em aprimorar as tecnologias no domínio militar, incluindo inteligência artificial (IA), dados massivos, computação em nuvem, computação quântica e internet das coisas (IoT, do inglês *internet of things*). Além disso, introduz uma inovação fundamental na estruturação de suas forças militares: Forças de Apoio Estratégico foram criadas para consolidar as missões estratégicas de guerra espacial, eletrônica e cibernética dos militares no sistema de operações conjuntas do Exército de Libertação Popular da China (Jiang, 2021).

Em termos da proteção de dados pessoais, várias agências governamentais chinesas aprovaram leis ou emitiram políticas, abrangendo desde leis nacionais, interpretações judiciais até regulamentos administrativos e padrões da indústria. No âmbito da legislação civil, o artigo 111 dos Princípios Gerais de Direito Civil da República Popular da China (2017)<sup>6</sup> estabelece bases para a proteção geral de informações pessoais. Da mesma forma, a Lei de Segurança Cibernética da China (2017)<sup>7</sup> contém disposições para regular a coleta, o armazenamento, a transmissão e o uso de “informações pessoais” por operadores de rede e operadores de infraestrutura crítica de informação. Além disso, essa lei exige a localização de dados para “operadores de infraestrutura de informação crítica”, tanto nacionais quanto estrangeiros. Em 2019, a Administração do Ciberespaço da China (ACC) lançou um projeto de Medidas Administrativas de Segurança de Dados com o objetivo de regular a coleta, o armazenamento, a transmissão, o processamento e o uso de dados pessoais no território chinês. Em relação à transferência transfronteiriça, em junho de 2019 foi divulgado um projeto de medidas sobre a avaliação de segurança da transferência transfronteiriça de informações pessoais. A Especificação de Segurança de Informações Pessoais (GB/T 35273-2020), publicada em 2020, é amplamente considerada a norma regulatória mais abrangente da China. Essa especificação inclui muitos elementos semelhantes às disposições do Regulamento Geral sobre a Proteção de Dados (RGPD), uma lei da União Europeia (UE) voltada para a proteção de dados pessoais de indivíduos. Além disso, a Especificação apresenta inovações, como o “Modelo de Política de Privacidade”, que oferece orientações práticas para as organizações na conformidade com os padrões de proteção de dados por meio de seus termos de serviço (Jiang, 2021).

---

<sup>4</sup> Estratégia Militar da China. **Xinhua**, 26 maio. 2015. Disponível em: [http://www.xinhuanet.com/politics/2015-05/26/c\\_1115408217.htm](http://www.xinhuanet.com/politics/2015-05/26/c_1115408217.htm)

<sup>5</sup> Defesa Nacional da China na Nova Era. **Xinhua**, 24 set. 2019. Disponível em: [https://www.gov.cn/zhengce/2019-07/24/content\\_5414325.htm](https://www.gov.cn/zhengce/2019-07/24/content_5414325.htm)

<sup>6</sup> Princípios Gerais de Direito Civil da República Popular da China. **Xinhua**, 18 mar. 2017. Disponível em: [https://www.gov.cn/xinwen/2017-03/18/content\\_5178585.htm#1](https://www.gov.cn/xinwen/2017-03/18/content_5178585.htm#1)

<sup>7</sup> Lei de Segurança Cibernética da China. **Xinhua**, 7 nov. 2016. Disponível em: [https://www.gov.cn/xinwen/2016-11/07/content\\_5129723.htm](https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm)

## Conceitos sobre crime cibernético

Os tipos mais comuns de cibercrimes no país são fraude financeira *online*, ataques ao ecossistema *online* e extensões de crimes *offline*, como pornografia *online* e jogos de apostas (Jiang, 2021). Consequentemente, a legislação dirigida ao cibercrime na China visa a resolver essas questões.

Já em 1997, os artigos 285, 286 e 287 do Direito Penal da República Popular da China reconheciam vários tipos de crimes cibernéticos. As Emendas VII (2009) e IX (2015) ao Direito Penal incorporaram mais crimes facilitados ou habilitados pela internet. Notavelmente, em 2015, a Emenda IX ao Direito Penal criminalizou a disseminação de “notícias falsas” *online*. A Lei de Segurança Cibernética da China (2017)<sup>8</sup> também contém várias disposições direcionadas aos operadores de infraestrutura de informação crítica que violam obrigações e deveres específicos, como a localização de dados que regem “informações pessoais” e “dados importantes”. A não conformidade pode resultar em multas de até 500.000 RMB (cerca de US\$ 71.000) e prisão de até cinco anos em casos graves. A Lei Antiterrorismo da China (2015)<sup>9</sup> tem regras específicas para que os provedores de serviços da internet removam e notifiquem conteúdo terrorista *online*. Várias interpretações judiciais e pareceres da Suprema Corte ampliaram o escopo em relação às extensões cibernéticas de crimes já proibidos pelo Direito Penal chinês, como pornografia *online* (2010), jogos de azar *online* (2010), difamação *online* (2013), processos criminais em casos de cibercrime (2014) e violação de informações pessoais (2017).

Além disso, o Ministério da Segurança Pública emitiu regulamentos relacionados, incluindo o Regulamento de Supervisão e Inspeção de Segurança Cibernética por Órgãos de Segurança Pública (2018) e as Regras sobre Obtenção de Dados Eletrônicos como Prova por Autoridades de Segurança Pública no Tratamento de Casos Criminais (2019). No entanto, tecnologias avançadas, como a IA e o reconhecimento facial, vêm sendo cada vez mais integradas ao sistema policial chinês. Atualmente, a China detém um imenso banco de dados de reconhecimento facial, que emprega a IA para identificar cidadãos em questão de segundos. Cientistas chineses desenvolveram uma câmera de reconhecimento facial com 500 *megapixels*. Essa câmera foi projetada para funcionar em conjunto com sistemas de vigilância, permitindo que captem rostos em meio a multidões, os quais podem ser posteriormente identificados por meio de *softwares* de IA.<sup>10</sup> Em 2020, Wang Yi, ministro dos Negócios Estrangeiros da República Popular da China, propôs a Iniciativa Global sobre Segurança de Dados no simpósio internacional intitulado “Aproveitando as oportunidades digitais para a cooperação e o desenvolvimento”. Em 2023, durante o discurso de abertura no 3º Fórum para Cooperação Internacional do Cinturão e Rota, o presidente chinês Xi Jinping propôs a Iniciativa Global de Governança de Inteligência Artificial. Essa iniciativa focaliza a cooperação global no que diz respeito à governança da IA na era da civilização digital. Ela representa a ação concreta da China na implementação ativa do conceito de comunidade do futuro compartilhado para a humanidade no domínio da IA, bem como na construção da Iniciativa de Desenvolvimento Global, Iniciativa de

<sup>8</sup> Lei de Segurança Cibernética da China. **Xinhua**, 7 nov. 2016. Disponível em: [https://www.gov.cn/xinwen/2016-11/07/content\\_5129723.htm](https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm)

<sup>9</sup> Lei Antiterrorismo da China. **Ministério da Justiça da China**, 25 dec. 2018. Disponível em: [https://www.moj.gov.cn/pub/sfbgw/flfggz/flfggzflty/fltysfxzsgflfg/201812/t20181225\\_151327.html](https://www.moj.gov.cn/pub/sfbgw/flfggz/flfggzflty/fltysfxzsgflfg/201812/t20181225_151327.html)

<sup>10</sup> GEORGE, C. A ‘super câmera’ chinesa de 500 megapixels pode detectar um rosto na multidão. **Digital Camera World**, 13 jul. 2020. Disponível em: <https://www.digitalcameraworld.com/news/chinese-500-megapixel-super-camera-can-spot-a-face-in-the-crowd>. Acesso em: 23 jan. 2025.

Segurança Global e Iniciativa de Civilização Global.<sup>11</sup> Em 2024, durante sua participação na 14ª Reunião dos Altos Representantes do Brics e Brics+ sobre Assuntos de Segurança, Wang Yi destacou que a China está disposta a trabalhar com o Brics para implementar integralmente a Iniciativa Global sobre Segurança de Dados e a Iniciativa Global de Governança de Inteligência Artificial, aprofundando continuamente a cooperação de segurança do Brics, de forma a construir em conjunto um mundo pacífico e tranquilo, dando início a um futuro mais promissor.<sup>12</sup>

### Conceitos sobre terrorismo cibernético

A regulamentação da China em relação ao terrorismo cibernético fundamenta-se, em grande parte, no Direito Penal da República Popular da China, com o apoio complementar da Lei Antiterrorismo da China e da Lei de Segurança Cibernética da China.

Desde o Anteprojeto do Direito Penal, de 1950, até o vigente Direito Penal, a legislação penal chinesa sofreu inúmeras emendas. O Direito Penal vigente regula, principalmente, crimes contra a segurança pública, crimes que prejudicam a ordem da administração pública e outros delitos relacionados aos crimes de terrorismo. Além disso, o Direito Penal também contém algumas disposições processuais que apoiam o direito substantivo. Embora o sistema legal para punir crimes de ciberterrorismo seja relativamente completo, as normas específicas para lidar com esses crimes são escassas. A Lei Antiterrorismo (2015)<sup>13</sup> se tornou uma lei de regulamentação especial para atos criminosos relacionados ao terrorismo. Nessa lei, as disposições sobre delitos terroristas são dispersas, e não havia cláusulas específicas sobre ciberterrorismo. No entanto, ela define as obrigações dos provedores de rede, fornece serviços técnicos para a investigação de casos, estabelece uma conexão eficaz com o Direito Penal e também tem papel significativo na luta contra o terrorismo e na regulamentação da criminalidade terrorista. Na Lei de Segurança Cibernética (2017)<sup>14</sup>, estão elencados os aspectos gerais referentes a infrações de ciberterrorismo, estando concentrados no artigo 12. Essa lei estabelece a base jurídica para a punição de crimes de ciberterrorismo, definindo o comportamento cibernético do Estado e dos indivíduos, e equilibrando os esforços de segurança nacional, segurança cibernética e luta contra o terrorismo. Contudo, as cláusulas de ciberterrorismo previstas na lei são de natureza administrativa e não estão diretamente relacionadas aos crimes de ciberterrorismo (Zeng; Wang, 2024).

Além disso, a China também publicou vários documentos legais. Em 2017, a Região Autônoma Uigur de Xinjiang introduziu o primeiro regulamento local chinês para conter e erradicar o extremismo religioso.<sup>15</sup> Esse regulamento introduziu os conceitos de extremismo e atividade extremista e definiu

<sup>11</sup> FEI Y.; ZHAO K. O significado mundial da iniciativa global de governança da inteligência artificial. **Rede da Ciência Social da China (CSSN)**, 19 jun. 2024. Disponível em: [https://www.cssn.cn/gjgc/mhgj/202406/t20240619\\_5759700.shtml](https://www.cssn.cn/gjgc/mhgj/202406/t20240619_5759700.shtml). Acesso em: 15 jan. 2025.

<sup>12</sup> WANG Yi propõe quatro iniciativas para os países BRICS trabalharem juntos para enfrentar ameaças de segurança. **Agência de Notícias Xinhua**, 11 set. 2024. Disponível em: <http://www.news.cn/20240911/1b77fa5016bf4fcbab0453944a9965c6/c.html>. Acesso em: 15 jan. 2025.

<sup>13</sup> Lei Antiterrorismo da China. **Ministério da Justiça da China**, 25 dec. 2018. Disponível em: [https://www.moj.gov.cn/pub/sfbgw/flfggz/flfggzflty/fltysfxzgxflfg/201812/t20181225\\_151327.html](https://www.moj.gov.cn/pub/sfbgw/flfggz/flfggzflty/fltysfxzgxflfg/201812/t20181225_151327.html)

<sup>14</sup> Lei de Segurança Cibernética da China. **Xinhua**, 7 nov. 2016. Disponível em: [https://www.gov.cn/xinwen/2016-11/07/content\\_5129723.htm](https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm)

<sup>15</sup> XINJIANG formula primeiro regulamento local chinês para eliminar extremismo religioso. **Português – People's Daily Online**, 31 mar. 2017. Disponível em: <http://portuguese.people.com.cn/n3/2017/0331/c309806-9197563.html>. Acesso em: 23 jan. 2025.

o grupo de liderança para a “desextremização” e suas funções de trabalho, fornecendo valiosa experiência no campo da luta contra o terrorismo internacional. A China também elaborou vários documentos legais, incluindo a Convenção da Organização para Cooperação de Xangai (OCX) sobre Combate ao Extremismo (2018) e a Lei da República Popular da China sobre a Salvaguarda da Segurança Nacional na Região Administrativa Especial de Hong Kong (2020).

### Conceitos sobre cibersegurança do Brics

Em 2017, foi lançada na 9ª Cúpula do Brics a Declaração de Xiamen, que esclarece a posição comum dos países do Brics na governança global do espaço cibernético. Ela reafirma e propõe de forma criativa um papel central das Nações Unidas na formulação de normas de comportamento responsável dos Estados no espaço cibernético, adotando como base os princípios do direito internacional, com a Carta das Nações Unidas em seu núcleo. Além disso, a declaração delinea um caminho para fortalecer a cooperação internacional e apresenta um Roteiro de Cooperação Prática do Brics para Garantir a Segurança no Uso de Tecnologias de Informação e Comunicação. É a primeira vez em que os países do Brics alcançam um alto grau de consenso sobre um código de conduta global para os Estados no ciberespaço.<sup>16</sup> Esse consenso se fundamenta nas normas de conduta no ciberespaço, que respeitam a igualdade soberana dos países, sendo a China e a Rússia as principais defensoras dessas normas. A partir de um conjunto de normas de conduta nacional responsável no ciberespaço, com as Nações Unidas como plataforma central, um conjunto de normas de conduta nacional responsável no ciberespaço global foi sistematicamente derivado. Em 2022, a 8ª Reunião do Grupo de Trabalho do Brics sobre Segurança Cibernética adotou por consenso o “Relatório de Progresso sobre Roteiro de Cooperação Prática do Brics para Garantir a Segurança no Uso de Tecnologias de Informação e Comunicação”. Esse relatório recapitula a experiência adquirida e o progresso alcançado pelo grupo de trabalho na implementação do roteiro ao longo dos últimos cinco anos. Além disso, os membros do grupo chegaram a um consenso crucial sobre a direção da cooperação futura no domínio da cibersegurança, estabelecendo um caminho sólido para o fortalecimento e a continuidade da colaboração entre os países do Brics nesse campo fundamental.

Em 2024, a Declaração de Kazan, publicada na 16ª Cúpula do Brics, incluiu várias referências à “cibersegurança”. Segundo ela, os países do Brics reconhecem os imensos desafios e ameaças no âmbito digital e expressam preocupação grave com o frequente uso malicioso das tecnologias de informação e comunicação, bem como com a proliferação de informações falsas. Enfatizam a importância de que as Nações Unidas tenham papel de liderança preponderante, e que a cooperação internacional entre os Estados seja fortalecida. Solicitam o desenvolvimento e a implementação de regras e padrões universais para a segurança da cadeia de suprimentos global. Além disso, reconhecem o progresso alcançado na promoção da cooperação do Brics de acordo com o Roteiro de Cooperação Prática do Brics para Garantir a Segurança no Uso de Tecnologias de Informação e Comunicação e seu relatório de progresso.<sup>17</sup> Como força representativa das economias emergentes, o Brics tem

<sup>16</sup> CONSTRUIR juntos a “BRICS Cibernética”: este pode ser o campo com maior expectativa de progressos significativos nos próximos dez anos. *The Paper*, 7 set. 2017. Disponível em: [https://m.thepaper.cn/kuaibao\\_detail.jsp?contid=1787142&from=kuaibao](https://m.thepaper.cn/kuaibao_detail.jsp?contid=1787142&from=kuaibao). Acesso em: 15 jan. 2025.

<sup>17</sup> BRASIL. Ministério das Relações Exteriores. Declaração de Kazan. In: CÚPULA DO BRICS, 16., 2024, Kazan, Rússia. **Declaração final**. Brasília, DF: Ministério das Relações Exteriores, 24 out. 2024. Disponível em: [https://www.gov.br/mre/pt-br/canais\\_atendimento/imprensa/notas-a-imprensa/xvi-cupula-do-brics-2013-kazan-russia-22-a-24-de-outubro-de-2024-declaração-final](https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/xvi-cupula-do-brics-2013-kazan-russia-22-a-24-de-outubro-de-2024-declaração-final). Acesso em: 15 jan. 2025.

expandido progressivamente sua influência internacional em áreas de segurança não tradicionais, como a cibersegurança. A China participa ativamente na promoção da formulação de regras internacionais pertinentes, fornecendo um código de conduta para a governança da segurança cibernética.

## PRÁTICAS DA CHINA NA GOVERNANÇA DA CIBERSEGURANÇA

A China é testemunha e beneficiária do desenvolvimento digital global. Desde seu acesso integral à internet internacional, em 1994, o país traçou um caminho de desenvolvimento de rede e informatização com suas próprias características e formou um ecossistema composto por muitas empresas de internet de classe mundial, como Huawei, ZTE, Alibaba, Tencent, Baidu e TikTok (Jiang, 2021), dando origem à maior e mais dinâmica sociedade digital do mundo. O 54º relatório estatístico sobre o desenvolvimento cibernético da China, divulgado pelo Centro de Informações da Rede de Internet da China (CNNIC), mostra que, até junho de 2024, o número de usuários de internet na China chegou a cerca de 1,1 bilhão, ocupando o primeiro lugar mundial, com taxa de penetração de 78%.<sup>18</sup> Em 2023, a escala da economia digital da China chegou a 53,9 trilhões de *yuan*s, representando 10% da produção global de dados, segundo o Relatório de Pesquisa sobre o Desenvolvimento da Economia Digital da China (2024).<sup>19</sup> Além disso, a China construiu a mais extensa e tecnologicamente pioneira infraestrutura de rede global, com redes 5G que alcançam todas as cidades e condados em áreas urbanas do país inteiro.

No entanto, juntamente com esse avanço, o país também enfrenta diversos tipos de riscos e desafios decorrentes do desenvolvimento das tecnologias de informação e comunicação. Diante dessa situação, tem insistido na integração de desenvolvimento e segurança, promovendo continuamente o desenvolvimento digital e elevando sua capacidade geral de segurança cibernética. As práticas da China na governança da cibersegurança são resumidas a seguir.

### Construção da sólida estrutura política para a cibersegurança

O governo chinês concentrou as decisões políticas relacionadas à cibersegurança em um regulador central: a Administração do Ciberespaço da China (ACC). A ACC, como órgão oficial responsável pela supervisão da internet na China, responde perante a Comissão Central de Assuntos do Ciberespaço. Essa comissão é uma agência interministerial governamental, liderada pelo presidente Xi Jinping e composta por altos dirigentes chineses. Criada em 2014, a ACC assumiu o controle da regulação da internet e estabeleceu 31 escritórios em nível provincial associados às atividades de propaganda e ao controle de conteúdo (Alsabah, 2016).

Além disso, foi elaborada e aprovada uma série de leis e políticas cibernéticas em diversos níveis. Tais iniciativas têm como objetivo atender às necessidades internas e responder às tendências geopolíticas e políticas externas. A China promulgou, sucessivamente, mais de 150 leis relacionadas à segurança

<sup>18</sup> CENTRO CHINÊS DE INFORMAÇÃO SOBRE A INTERNET E A REDE (CNNIC). **Relatório estatístico sobre o desenvolvimento da internet em China**. 54. ed. [S. l.: s. n.], [20--?].

<sup>19</sup> ACADEMIA CHINESA DE TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO (CAICT). **Relatório de estudo sobre o desenvolvimento da economia digital da China**. [S. l.: s. n.], 2024.

cibernética,<sup>20</sup> incluindo a Lei de Segurança Cibernética, a Lei de Segurança de Dados e a Lei de Proteção de Informações Pessoais. Além disso, emitiu mais de 300 normas nacionais sobre cibersegurança.<sup>21</sup> A fim de promover o livre e ordenado fluxo de dados, enquanto protege a segurança dos dados, a China emitiu as Disposições sobre a Promoção e o Regulamento do Fluxo Transfronteiriço de Dados. Com o objetivo de fortalecer a governança abrangente dos algoritmos em serviços de informação na internet e promover o desenvolvimento padronizado e saudável dos serviços de recomendação algorítmica, lançou as Disposições sobre a Recomendação de Algoritmos de Serviço de Informações Baseadas na Internet. Para implementar a Iniciativa Global de Governança de Inteligência Artificial e reforçar a governança da segurança da IA, a China introduziu as Medidas Provisórias para Regular Serviços de Inteligência Artificial Generativa, a primeira legislação especial do mundo sobre IA generativa. Além disso, emitiu a Estrutura de Governança de Segurança sobre Inteligência Artificial, que apresenta princípios na gestão da segurança da IA.

Ovchinnikova e Upadhyay (2023) descobriram que o nível de segurança cibernética está diretamente relacionado ao grau de responsabilidade assumido pelo Estado. Por exemplo, os países com regulamentação governamental mais robusta, como a Rússia e a China, apresentam um nível mais elevado de segurança cibernética. Por outro lado, os países com sistemas de defesa cibernética insuficientemente centralizados ocupam posições mais baixas na classificação, como o Brasil, a África do Sul e a Índia, e são frequentemente alvos de ataques cibernéticos. Portanto, chegamos à conclusão de que as práticas chinesas de fortalecimento do controle estatal sobre a segurança cibernética já atingiram notáveis êxitos.

### **Estabelecimento da infraestrutura de comunicações digitais**

A China adere firmemente à filosofia de desenvolvimento centrado nas pessoas. Seu objetivo principal é garantir que as informações e os serviços digitais sejam acessíveis, economicamente viáveis e eficazes, de modo a beneficiar a população em sua totalidade. O país vem avançando continuamente na construção de infraestruturas digitais, como a rede 5G, a rede de banda larga de fibra óptica, o IPv6, o Sistema de Navegação por Satélite Beidou, ou BDS, e a computação em nuvem. Por exemplo, até o momento, a China construiu e tornou operacionais mais de 4,1 milhões de estações de base 5G, criando a maior rede 5G de grupo independente do mundo. Simultaneamente, com base na infraestrutura da rede 5G, foi construída uma nova plataforma de aplicativos comerciais 5G/6G baseada na nuvem, e se formou uma nova rede de inteligência digital para a indústria avançada da internet industrial.<sup>22</sup> Essa evolução tecnológica tem sido um catalisador para o desenvolvimento acelerado do setor de IA. Além disso, a internet dos veículos (IoV, do inglês *internet of vehicles*), a IoT e a internet industrial têm se expandido e desenvolvido vigorosamente. Esses avanços tecnológicos têm dado origem a uma rede e um espaço digital em que todos os elementos estão interconectados, as interações entre pessoas e máquinas são harmoniosas e a integração entre o domínio terrestre e o

<sup>20</sup> CHINA promulga mais de 150 leis na área de internet. **Agência de Notícias Xinhua**, 18 jun. 2024. Disponível em: <http://www3.xinhuanet.com/legal/20240618/349e591deb584fb688fa896b37e7cbd2/c.html#:~:text=%E6%96%B0%E5%8D%8E%E7%A4%BE%E5%8C%97%E4%BA%AC6%E6%9C%881,%E5%9D%9A%E5%AE%9E%E7%9A%84%E5%88%B6%E5%BA%A6%E4%BF%9D%E9%9A%9C%E3%80%82>. Acesso em: 16 jan. 2025.

<sup>21</sup> RELATO da trajetória da segurança cibernética em China sob a orientação do secretário geral Xi Jinping. **China Cyberspace**, [s. l.], n. 6, p. 4-14, 2022.

<sup>22</sup> ZENG, J. Q. A construção da infraestrutura de informação digital continua a ser ponto principal de ação. **People's Post and Telecommunications**, 26 dez. 2024. Disponível em: [https://www.cnii.com.cn/rmydb/202412/t20241226\\_626664.html](https://www.cnii.com.cn/rmydb/202412/t20241226_626664.html). Acesso em: 15 jan. 2025.

celeste está cada vez mais evidente. Essa realidade digital abrange desde as comunicações cotidianas até as aplicações mais avançadas em diversos setores, proporcionando uma base sólida para o desenvolvimento econômico, social e tecnológico contínuo da China.

Reconhecendo a particular fragilidade da indústria de segurança cibernética do país, o governo chinês promove e investe ativamente no crescimento de seu mercado de segurança de rede. Por exemplo, defende a estratégia de “fusão militar-civil”, com o objetivo de fortalecer a sinergia entre as esferas militar e civil. Dessa forma, as forças militares chinesas podem beneficiar-se diretamente dos avanços tecnológicos em várias áreas, incluindo computação em nuvem, robótica, aviação, tecnologia nuclear e outras. Além disso, por meio da OCX, a China tem realizado exercícios com o intuito de se preparar para o ciberterrorismo externo e os ataques cibernéticos. Os exercícios de defesa cibernética em nível estatal sempre foram considerados essenciais para a preparação da defesa cibernética. Isso fortalece a capacidade de resposta às ameaças cibernéticas e promove a cooperação e a troca de experiências entre os membros da OCX, contribuindo para a construção de um ambiente mais seguro e estável no ciberespaço global.

O avanço da infraestrutura digital tem papel crucial na elevação do nível de desenvolvimento das novas forças produtivas de qualidade nas cidades (Lu; Wang; Guo, 2024), propiciando o impulso ao desenvolvimento econômico de alta qualidade (Huang, 2024). O estudo do Zhou (2022) indica que o desenvolvimento da internet móvel na China impulsionou o rápido crescimento da economia digital no país, fornecendo uma garantia fundamental para o crescimento econômico chinês nas próximas décadas.

### Promoção do desenvolvimento do setor de cibersegurança

De acordo com as estatísticas do Relatório de Análise do Setor de Cibersegurança da China (2024), o tamanho do mercado de segurança de rede da China alcançou aproximadamente 64 bilhões de *yuan*s, com taxa de crescimento de cerca de 1,1%.<sup>23</sup> A escala do mercado de segurança cibernética chinês tem expandido progressivamente. As empresas de segurança cibernética já cobrem, basicamente, sete áreas fundamentais, incluindo a rede e a infraestrutura, o desenvolvimento e a segurança de dados. Para garantir a ordem pública, o governo chinês tem investido consideráveis recursos no policiamento cibernético, incluindo programas de vigilância de alta tecnologia, como o sistema de crédito social. Em agosto de 2015, o Ministério da Segurança Pública implantou departamentos nacionais de segurança pública em *sites* e empresas da internet, criando o “Escritório de Polícia de Segurança da Internet”. Entre 2015 e 2017, o país concluiu a construção de 1.116 “unidades policiais de cibersegurança”. Em *sites* importantes, como *Baidu*, *Tencent*, *Sina* e outros grandes portais, foram construídas “unidades policiais de cibersegurança” de primeiro nível. Além disso, foram selecionados 63 exemplares de “unidades policiais de cibersegurança”.<sup>24</sup> Essas iniciativas têm obtido resultados notáveis na manutenção da segurança cibernética e na proteção dos direitos e interesses dos usuários da internet.

<sup>23</sup> ALIANÇA DA INDÚSTRIA DE SEGURANÇA CIBERNÉTICA DA CHINA (CCIA). **Relatório de análise da indústria de segurança cibernética da China (2024)**. [S. l.: s. n.], 2024.

<sup>24</sup> CAI, C. Milhões de centros policiais de segurança cibernética foram construídos nacionalmente, e 30,7 bilhões de registros de informações pessoais foram sequestrados. **Diário Jurídico**, 14 fev. 2017. Disponível em: [https://www.thepaper.cn/newsDetail\\_forward\\_1618094](https://www.thepaper.cn/newsDetail_forward_1618094). Acesso em: 23 jan. 2025.

Em termos de educação, mais de 90 faculdades e universidades na China instituíram faculdades especializadas em cibersegurança, enquanto mais de 200 faculdades e universidades criaram cursos nesse campo. Isso contribuiu para acelerar a formação de um ecossistema benéfico para o cultivo de talentos, a inovação tecnológica e o desenvolvimento industrial da segurança cibernética. Essa articulação entre o setor acadêmico e o mercado econômico promove a consolidação e o avanço contínuo do setor de cibersegurança na China, garantindo a capacidade de enfrentar os desafios cibernéticos presentes e futuros.

O governo chinês lançou várias políticas industriais abrangentes para impulsionar as capacidades tecnológicas do país. Em 2015, foi divulgado o plano “*Internet Plus*”, que busca modernizar os setores tradicionais do país, desde a agricultura até a indústria de manufatura. Além disso, no mesmo ano, a “Rota da Seda Digital” foi adotada como parte da iniciativa “Cinturão e Rota”. Seu objetivo é explorar novos mercados tecnológicos em todo o mundo, o que envolve a atualização da infraestrutura da internet, a adoção de padrões tecnológicos comuns e o aprimoramento dos sistemas de policiamento. O plano “*Made in China 2025*” visa a transformar a China da fábrica mundial de produtos baratos em uma nação que produz produtos e serviços de maior valor agregado. Essas iniciativas são fundamentais para a expansão global da influência tecnológica da China e para a promoção do desenvolvimento econômico e tecnológico em escala internacional.

Sob a influência conjunta da orientação política, da demanda, da tecnologia e de outros fatores impulsores, o setor de cibersegurança da China apresenta uma tendência de desenvolvimento vigoroso. Com os esforços ativos do governo, do setor privado, do meio acadêmico, da comunidade de pesquisa e do mercado de investimento, a capacidade de fornecimento do setor de segurança cibernética do país tem aumentado consistentemente. Prevê-se que o setor de cibersegurança da China continue a se desenvolver de forma estável e positiva no futuro. A vitalidade do mercado continuará a se fortalecer, a estrutura industrial seguirá sendo otimizada, e a fusão de novas tecnologias dará origem a novos produtos e serviços, remodelando as vantagens competitivas do setor (Ying; Zhao, 2024).

## PERSPECTIVAS DA COOPERAÇÃO DO BRICS NA CIBERSEGURANÇA

Nos últimos anos, os países membros do Brics, economias emergentes, enfrentam oportunidades e desafios comuns no domínio cibernético. Essa realidade estabelece uma sólida base estratégica para a cooperação em cibersegurança no seio do bloco. O caso de Edward Snowden, ocorrido em 2013, tornou-se um importante catalisador para a cooperação em cibersegurança entre os países do bloco. Desde então, essa cooperação tem demonstrado progressos notáveis. No entanto, ainda existem um vasto espaço e potencial para serem explorados em termos de cooperação.

Primeiramente, é imperativa a harmonização de políticas e regulamentações em segurança cibernética entre os países do Brics. A transformação digital que a interação entre os membros do grupo sofreu elevou significativamente sua capacidade de colaboração econômica e potencializou a elaboração de uma estratégia conjunta de segurança cibernética. Conforme concluído por Ovchinnikova e Upadhyay (2023), o controle estatal sobre o ciberespaço e a existência de estratégias nacionais sólidas são pré-requisitos indispensáveis para alcançar um alto nível de cibersegurança. Isso sublinha a

importância fundamental da coordenação entre as políticas nacionais de segurança cibernética dos países do Brics, uma vez que é crucial para enfrentar os desafios comuns no domínio cibernético, fortalecer a defesa coletiva e garantir a estabilidade e o desenvolvimento econômico e social desses países.

Quando se trata de cooperação internacional no ciberespaço, a China sempre adere firmemente ao conceito de construir uma comunidade de destino, promovendo ativamente a colaboração internacional nesse domínio. Em 2017, o país lançou sua Estratégia Internacional da Cooperação no Ciberespaço, estabelecendo os princípios fundamentais, os objetivos estratégicos e os planos de ação para sua participação na cooperação internacional no ciberespaço. Desde então, a China se envolveu profundamente no processo de segurança cibernética do Brics, aprofundando a comunicação política e a cooperação prática com os países-membros do bloco. Embora existam vários tratados internacionais que abrangem a segurança do espaço cibernético, ainda não há uma agenda coerente e unificada entre os países membros do Brics nesse domínio (Wang, 2022). Portanto, é essencial que os países do grupo considerem de forma abrangente os interesses e as preocupações de todas as partes envolvidas. Devem-se envidar esforços para aumentar a vontade política e alcançar consenso sobre a governança no âmbito dos mecanismos multilaterais, com o objetivo de promover a formulação de regras internacionais universalmente aceitas para o ciberespaço e a elaboração de uma convenção internacional sobre o contraterrorismo no ciberespaço, apoiadas nas estruturas e no quadro normativo das Nações Unidas.

Em segundo lugar, é crucial a construção de uma infraestrutura global de informações interconectada. Conforme Belli (2019), apenas com infraestruturas e serviços acessíveis e seguros é possível aproveitar plenamente as enormes oportunidades proporcionadas pelos avanços tecnológicos. Dessa forma, a proteção e a segurança das infraestruturas modernas se tornam questões fundamentais para o desenvolvimento dos países do Brics, uma vez que eles investem intensivamente na digitalização e no potencial de tecnologias interconectadas e interdependentes, tais como a 5G e a IoT.

A China está profundamente empenhada na promoção da interconexão e intercomunicação da infraestrutura global de informações. Ao longo dos anos, envolveu-se ativamente na construção de mais de 130 conjuntos de cabos terrestres transfronteiriços.<sup>25</sup> Por intermédio de plataformas estratégicas, como a Reunião de Ministros das Comunicações do Brics e o Fórum do Brics sobre Parceria na Nova Revolução Industrial, a China tem dado um forte impulso aos intercâmbios e à cooperação com os países do Sul Global no domínio da segurança cibernética e da economia digital. Ao fortalecer esses laços de cooperação, demonstra seu papel ativo e responsável na construção de um ciberespaço mais seguro, conectado e próspero para todos.

Atualmente, o Brasil, a Índia e a África do Sul enfrentam consideráveis desafios no desenvolvimento da infraestrutura de informação e comunicação. De acordo com Ovchinnikova e Upadhyay (2023), fatores como a escassez de recursos, a complexidade geográfica e a carência de políticas eficazes dificultam o progresso nesse campo. Nesse contexto, a construção de redes de fibra óptica emerge como uma área de cooperação econômica altamente promissora entre os países do Brics. As tecnologias de fibra óptica permitem a transmissão de dados com alta velocidade e confiabilidade,

---

<sup>25</sup> ZHAO, Y. Reduzir o “abismo digital” e acelerar a construção da “Rota Digital da Seda”. **Rede Guangming**, 4 jan. 2024. Disponível em: [https://news.gmw.cn/2024-01/04/content\\_37069842.htm](https://news.gmw.cn/2024-01/04/content_37069842.htm). Acesso em: 17 jan. 2025.

elementos fundamentais para o desenvolvimento digital e econômico. A China e a Rússia, dotadas de experiência e *expertise* no setor, podem compartilhar conhecimentos, tecnologia e recursos com os demais países-membros do Brics. A troca de tecnologias e o desenvolvimento comum na construção de redes de fibra óptica não apenas contribuirão para a criação de um ecossistema digital mais robusto e integrado, abrindo caminho para inúmeras oportunidades de negócios e inovação, mas também ajudarão a superar as barreiras ao desenvolvimento da infraestrutura de informação e comunicação nesses países. Além disso, essa cooperação fortalecerá as relações econômicas e políticas entre os países do bloco.

Em terceiro lugar, é essencial a criação de um eficaz mecanismo de comunicação. Embora os países do Brics compartilhem prioridades e objetivos comuns no domínio da segurança cibernética, ainda carecem de estrutura coerente para o intercâmbio de inteligência (Malatji; Matli, 2023). Diante disso, a construção de uma cooperação sólida e multinacional, que permita que os países do grupo estabeleçam diálogos contínuos e recebam *feedbacks* valiosos, configura-se como estratégia altamente proveitosa para todos os envolvidos. Um passo ainda mais significativo seria a inclusão de governos, acadêmicos, representantes do setor privado e da sociedade civil dos países participantes, visando a alcançar uma coerência multisetorial. Essa abordagem integrativa possibilita a conjugação de diferentes perspectivas e *expertises*, enriquecendo o processo de tomada de decisão e a formulação de estratégias.

No que diz respeito à concretização dessa cooperação, o fortalecimento do estabelecimento de mecanismos de cooperação entre *think tanks* e centros de pesquisa sobre segurança cibernética se revela fundamental. Um exemplo ilustrativo é o projeto CyberBRICS, sediado pelo Centro de Tecnologia e Sociedade da Faculdade de Direito da Fundação Getulio Vargas (CTS-FGV), no Rio de Janeiro. Esse projeto é desenvolvido em parceria com a Escola Superior de Economia, em Moscou; a Jindal Global Law School e o Centro de Internet e Sociedade, na Índia; a Universidade Fudan, em Xangai; a Universidade de Hong Kong; e a Universidade Nelson Mandela e o Research ICT Africa, na África do Sul. A expansão e o aprofundamento de parcerias desse tipo podem propiciar o compartilhamento de conhecimento, a identificação de tendências emergentes no ciberespaço e a elaboração de estratégias conjuntas para enfrentar ameaças cibernéticas. Em última análise, a criação de um ecossistema de cooperação abrangente e dinâmico no campo da segurança cibernética é fundamental para o fortalecimento da defesa coletiva dos países do Brics e para o desenvolvimento de um ciberespaço mais seguro e estável.

No futuro, a China permanece disposta a manter sua colaboração ativa com os países do Brics, para formular regras e tratados sobre o ciberespaço, construir infraestrutura global de informações interconectada, bem como criar mecanismos de comunicação. Espera-se que todas essas ações possam não apenas contribuir diretamente para a segurança e a estabilidade cibernética do bloco do Brics, mas também ter impacto positivo na construção de um ciberespaço mais seguro, coeso e equilibrado em nível global.

## CONCLUSÕES

Na era digital em que vivemos, o avanço acelerado das novas tecnologias impõe desafios sem precedentes aos países-membros do Brics. Eles enfrentam desafios comuns, tais como ataques, crimes e terrorismo cibernéticos, que ameaçam a segurança e o desenvolvimento econômico e social.

Diante desse cenário, o governo chinês elaborou diversos conceitos para combater essas ameaças. Isso inclui leis como a Lei Antiterrorismo da China (2015), os Princípios Gerais de Direito Civil da República Popular da China (2017), a Lei de Segurança Cibernética da China (2017) e o Direito Penal da República Popular da China, bem como outras políticas, como a Estratégia Militar da China (2015), a Estratégia Internacional da Cooperação no Ciberespaço (2016), o Regulamento de Supervisão e Inspeção de Segurança Cibernética por Órgãos de Segurança Pública (2018), a Defesa Nacional da China na Nova Era (2019), a Especificação de Segurança de Informações Pessoais (2020), entre outras.

Com base nessas políticas, a China vem se esforçando na construção de uma sólida estrutura política para a cibersegurança, na ampliação da infraestrutura de comunicações digitais e na promoção do desenvolvimento do setor de cibersegurança. Isso impulsiona o desenvolvimento digital e fortalece a capacidade geral de segurança cibernética da China.

As práticas adotadas pela China podem ser valiosas experiências para os demais países do Brics. Além disso, a cooperação em segurança cibernética entre os países do bloco se mostra crucial, especialmente nas áreas da harmonização de políticas e regulamentações, na construção de infraestrutura global de informações interconectada e no estabelecimento de um eficaz mecanismo de comunicação.

É de esperar que essas ações contribuam diretamente para a segurança e a estabilidade cibernética do bloco, exercendo impacto positivo na construção de um ciberespaço mais seguro, coeso e equilibrado em nível global. Dessa forma, os países do Brics podem enfrentar as ameaças cibernéticas de forma conjunta, fortalecendo a resiliência e o desenvolvimento compartilhado em um mundo cada vez mais digital e interconectado.

## REFERÊNCIAS

- ACADEMIA CHINESA DE TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO (CAICT). **Relatório de estudo sobre o desenvolvimento da economia digital da China**. [S. l.: s. n.], 2024.
- ALIANÇA DA INDÚSTRIA DE SEGURANÇA CIBERNÉTICA DA CHINA (CCIA). **Relatório de análise da indústria de segurança cibernética da China (2024)**. [S. l.: s. n.], 2024.
- ALSABAH, N. Information control 2.0: the cyberspace administration of China tames the internet. **Mercator Institute for China Studies**, 18 maio 2016. Merics China Monitor. Disponível em: [https://merics.org/sites/default/files/2020-05/MERICS\\_China\\_Monitor\\_32\\_Eng.pdf](https://merics.org/sites/default/files/2020-05/MERICS_China_Monitor_32_Eng.pdf). Acesso em: 17 jan. 2025.
- BARRETO, E. M. Terrorismo cibernético e cenários especulativos. **Revista Brasileira de Inteligência**, v. 3, n. 4, p. 63-76, 2007.
- BELLI, L. 5G e IoT: BRICS precisam de cooperação em cibersegurança. **Convergência Digital**, 9 set. 2019.
- BRASIL. Ministério das Relações Exteriores. Declaração de Kazan. In: CÚPULA DO BRICS, 16., 2024, Kazan, Rússia. **Declaração final**. Brasília, DF: Ministério das Relações Exteriores, 24 out. 2024. Disponível em: [https://www.gov.br/mre/pt-br/canais\\_atendimento/imprensa/notas-a-imprensa/xvi-cupula-do-brics-2013-kazan-russia-22-a-24-de-outubro-de-2024-declaracao-final](https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/xvi-cupula-do-brics-2013-kazan-russia-22-a-24-de-outubro-de-2024-declaracao-final). Acesso em: 15 jan. 2025.
- CAI, C. Milhões de centros policiais de segurança cibernética foram construídos nacionalmente, e 30,7 bilhões de registros de informações pessoais foram sequestrados. **Diário Jurídico**, 14 fev. 2017. Disponível em: [https://www.thepaper.cn/newsDetail\\_forward\\_1618094](https://www.thepaper.cn/newsDetail_forward_1618094). Acesso em: 23 jan. 2025.
- CENTRO CHINÊS DE INFORMAÇÃO SOBRE A INTERNET E A REDE (CNNIC). **Relatório estatístico sobre o desenvolvimento da internet em China**. 54. ed. [S. l.: s. n.], [20--?].
- CHINA promulga mais de 150 leis na área de internet. **Agência de Notícias Xinhua**, 18 jun. 2024. Disponível em: <http://www3.xinhuanet.com/legal/20240618/349e591deb584fb688fa896b37e7cbd2/c.html#:~:text=%E6%96%B0%E5%8D%8E%E7%A4%BE%E5%8C%97%E4%BA%AC6%E6%9C%881,%E5%9D%9A%E5%AE%9E%E7%9A%84%E5%88%B6%E5%BA%A6%E4%BF%9D%E9%9A%9C%E3%80%82>. Acesso em: 16 jan. 2025.
- CONSTRUIR juntos a “BRICS Cibernética”: este pode ser o campo com maior expectativa de progressos significativos nos próximos dez anos. **The Paper**, 7 set. 2017. Disponível em: [https://m.thepaper.cn/kuaibao\\_detail.jsp?contid=1787142&from=kuaibao](https://m.thepaper.cn/kuaibao_detail.jsp?contid=1787142&from=kuaibao). Acesso em: 15 jan. 2025.
- FEI, Y.; ZHAO, K. O significado mundial da iniciativa global de governança da inteligência artificial. **Rede da Ciência Social da China (CSSN)**, 19 jun. 2024. Disponível em: [https://www.cssn.cn/gjgc/mhgj/202406/t20240619\\_5759700.shtml](https://www.cssn.cn/gjgc/mhgj/202406/t20240619_5759700.shtml). Acesso em: 15 jan. 2025.
- GAO, W. L. BRICS cybersecurity cooperation: achievements and deepening paths. **China Int'l Stud.**, p. 124-139, 2018.

GEORGE, C. A 'super câmera' chinesa de 500 megapixels pode detectar um rosto na multidão. **Digital Camera World**, 13 jul. 2020. Disponível em: <https://www.digitalcameraworld.com/news/chinese-500-megapixel-super-camera-can-spot-a-face-in-the-crowd>. Acesso em: 23 jan. 2025.

HUANG, P. Análise da diferença espaciotemporal da construção da infraestrutura digital urbana: baseado em dados de painel de 30 províncias da China. **Value Engineering**, n. 35, p. 5-7, 2024.

INSTITUTE FOR ECONOMICS & PEACE. **Global terrorism index 2024**. [s. l.: s. n.], 2024.

JIANG, M. Cybersecurity policies in China. In: BELLI, L. (org.). **CyberBRICS: cybersecurity regulations in the BRICS countries**. Switzerland: Springer, 2021. p. 183-226.

LI, Z. **Estudo sobre a governança do direito internacional e o plano chinês dos ataques cibernéticos**. 2023. Tese (Doutorado em Relações Internacionais e Estudos Regionais) – School of International Relations and Diplomacy, Beijing Foreign Studies University, Beijing, 2023. Disponível em:

[https://oversea.cnki.net/KCMS/detail/detail.aspx?dbcode=CDFD&dbname=CDFDLAST2024&filename=1023063126.nh&uniplatform=OVERSEA&v=GRshRwkYyrRul2naS43u5PUKct-5HG7kr9Nne8CbUQqaaXqsZ\\_AgCC8xF0rBvVHg](https://oversea.cnki.net/KCMS/detail/detail.aspx?dbcode=CDFD&dbname=CDFDLAST2024&filename=1023063126.nh&uniplatform=OVERSEA&v=GRshRwkYyrRul2naS43u5PUKct-5HG7kr9Nne8CbUQqaaXqsZ_AgCC8xF0rBvVHg). Acesso em: 23 jan. 2025.

LU, J.; WANG, Y. P.; GUO, Z. A. Impacto da construção da infraestrutura digital no desenvolvimento das novas forças produtivas. **Shanghai Economic Review**, n. 12, p. 16-29, 2024. DOI: 10.19626/j.cnki.cn31-1163/f.2024.12.001.

MALATJI, M.; MATLI, W. The potential benefits and challenges of a BRICS+ agency for cybersecurity intelligence exchange. **Journal of Information Security and Cybercrimes Research**, v. 6, n. 2, p. 116-129, 2023.

OVCHINNIKOVA, O.; UPADHYAY, N. K. The level of cybersecurity of the BRICS member countries in international ratings: prospects for cooperation. **BRICS Law Journal**, v. 10, n. 1, p. 7-34, 2023.

RELATO da trajetória da segurança cibernética em China sob a orientação do secretário geral Xi Jinping. **China Cyberspace**, [s. l.], n. 6, p. 4-14, 2022.

SILVA, A. R. I. (org.). **Crimes cibernéticos**. Porto Alegre: Livraria Casa do Advogado, 2018.

TSAGOURIAS, N. Cyber attacks, self-defence and the problem of attribution. **Journal of Conflict and Security Law**, v. 17, n. 2, p. 229-244, 2012.

WANG, R. P. Novas perspectivas para a cooperação de segurança cibernética dos países BRICS na era 5G. **Country and Regional Studies (Z1)**, p. 30-47, p. 172, 2022.

WANG Yi propõe quatro iniciativas para os países BRICS trabalharem juntos para enfrentar ameaças de segurança. **Agência de Notícias Xinhua**, 11 set. 2024. Disponível em: <http://www.news.cn/20240911/1b77fa5016bf4fcaba0453944a9965c6/c.html>. Acesso em: 15 jan. 2025.

XINJIANG formula primeiro regulamento local chinês para eliminar extremismo religioso. **Português – People's Daily Online**, 31 mar. 2017. Disponível em: <http://portuguese.people.com.cn/n3/2017/0331/c309806-9197563.html>. Acesso em: 23 jan. 2025.

YING, F. F.; ZHAO, Z. Estudo sobre a situação de desenvolvimento da indústria de segurança cibernética em China. **Guangdong Communications Technology**, n. 4, p. 7-10, 2024.

ZENG, J. Q. A construção da infraestrutura de informação digital continua a ser ponto principal de ação. **People's Post and Telecommunications**, 26 dez. 2024. Disponível em: [https://www.cnii.com.cn/rmydb/202412/t20241226\\_626664.html](https://www.cnii.com.cn/rmydb/202412/t20241226_626664.html). Acesso em: 15 jan. 2025.

ZENG, L.; WANG, Z. H. Governança jurídica do crime de terrorismo cibernético no contexto da era digital. **Journal of China Criminal Police University**, n. 1, p. 88-96, 2024. DOI: 10.14060/j.issn.2095-7939.2024.01.009.

ZHAO, Y. Reduzir o “abismo digital” e acelerar a construção da “Rota Digital da Seda”. **Rede Guangming**, 4 jan. 2024. Disponível em: [https://news.gmw.cn/2024-01/04/content\\_37069842.htm](https://news.gmw.cn/2024-01/04/content_37069842.htm). Acesso em: 17 jan. 2025.

ZHOU, A. Digital infrastructure and economic growth: evidence for China. **Journal of Infrastructure, Policy and Development**, v. 6, n. 1, p. 1397, 2022.